Dialogic®

# Dialogic® DSI Signaling Servers

## Signaling Web Server (SWS) Mode User Manual

## Copyright and Legal Notice

Copyright© 2010-2011 Dialogic Corporation. All Rights Reserved. You may not reproduce this document in whole or in part without permission in writing from Dialogic Corporation at the address provided below.

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Corporation or its subsidiaries ("Dialogic"). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic corporation at the address indicated below or on the web at www.dialogic.com.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 9800 Cavendish Blvd., 5th Floor, Montreal, Quebec, Canada H4M 2V9. **Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.**

Dialogic, Dialogic Pro, Dialogic Blue, Veraz, Brooktrout, Diva, Diva ISDN, Making Innovation Thrive, Video is the New Voice, Diastar, Cantata, TruFax, SwitchKit, SnowShore, Eicon, Eicon Networks, NMS Communications, NMS (stylized), Eiconcard, SIPcontrol, TrustedVideo, Exnet, EXS, Connecting to Growth, Fusion, Vision, PowerMedia, PacketMedia, BorderNet, inCloud9, I-Gate, Hi-Gate, NaturalAccess, NaturalCallControl, NaturalConference, NaturalFax and Shiva, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Inc. and its affiliates or subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 926 Rock Avenue, San Jose, California 95131 USA. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

The names of actual companies and products mentioned herein are the trademarks of their respective owners.

Any use case(s) shown and/or described herein represent one or more examples of the various ways, scenarios or environments in which Dialogic® products can be used. Such use case(s) are non-limiting and do not represent recommendations of Dialogic as to whether or how to use Dialogic products.

Publication Date: April 2011

Document Number: 64-1149-03

# Contents


**1 Overview** ..... 11
- 1.1 General Description ..... 11
- 1.2 Key Benefits ..... 11
  - 1.2.1 Other Operating Modes ..... 12
- 1.3 Related Information ..... 12
- 1.4 Applicability ..... 13
- 1.5 Hardware Overview ..... 13
  - 1.5.1 Part Numbers ..... 13
- 1.6 Signaling Overview ..... 13
- 1.7 Functional Summary ..... 13
  - 1.7.1 SWS Mode Overview ..... 13
  - 1.7.2 Application Software ..... 14
  - 1.7.3 Fault Monitoring ..... 14
    - 1.7.3.1 Diagnostic Log Files ..... 14
  - 1.7.4 Management Interface ..... 14
  - 1.7.5 IP Security ..... 14

**2 Specification** ..... 17
- 2.1 Hardware Specification ..... 17
- 2.2 Software Licenses ..... 17
  - 2.2.1 Software Licenses for SS7G31 and SS7G32 ..... 17
- 2.3 Capabilities ..... 19
  - 2.3.1 SS7G31 and SS7G32 Signaling Servers Protocol Capabilities ..... 19
  - 2.3.2 Application Interfaces ..... 19

**3 Architecture** ..... 21
- 3.1 Overview ..... 21
- 3.2 Signaling Topologies ..... 21
- 3.3 Multiple Network Support ..... 24
  - 3.3.1 Support for Multiple Local Point Codes ..... 25
  - 3.3.2 Support for Multiple Networks ..... 26
  - 3.3.3 Protocol Handling for Multiple Network Contexts ..... 27
    - 3.3.3.1 MTP Applications ..... 27
    - 3.3.3.2 SCCP Applications ..... 27
    - 3.3.3.3 TCAP/MAP Applications ..... 28
- 3.4 Inter-SWS Communication ..... 28
- 3.5 Transaction-Based Applications ..... 28
  - 3.5.1 Management of Local SCCP Sub-Systems ..... 28
- 3.6 Resilience ..... 29
  - 3.6.1 IP Resilience ..... 29
- 3.7 Management Reporting ..... 29
- 3.8 Alarms ..... 29

**4 Licensing, Installation and Initial Configuration** ..... 31
- 4.1 Software Licensing ..... 31
  - 4.1.1 Purchasing Software Licenses ..... 31
  - 4.1.2 Temporary Licenses ..... 32
  - 4.1.3 Trial Licenses ..... 32
- 4.2 Installing the SWS Unit ..... 32
  - 4.2.1 Connecting a VT100 Terminal ..... 32
  - 4.2.2 IP Configuration ..... 33
  - 4.2.3 Software Download ..... 34
  - 4.2.4 Installing Software Licenses ..... 35
  - 4.2.5 Configuration Procedure ..... 35

**5 System Management** ..... 37
5.1 Management Interfaces ..... 37
5.2 System Software ..... 37
5.2.1 Updating the Software by FTP Transfer ..... 37
5.2.2 Updating the software from USB (SS7G31 and SS7G32 Systems) ..... 38
5.3 Diagnostics ..... 38
5.4 SNMP ..... 39
5.4.1 Overview ..... 39
5.4.2 DSMI SNMP ..... 39
5.5 Alarm Listing ..... 40
5.6 Hard Disk Management ..... 41
5.6.1 SS7G31 and SS7G32 Hard Disk Drive RAID Management ..... 41
5.7 Secure Shell (SSH) ..... 42
5.7.1 Configuring Public-Key Authentication for SSH ..... 43
5.7.2 SSH Tunneling for RSI ..... 43
5.7.2.1 Using Linux and OpenSSH ..... 43
5.7.2.2 Using Windows and PuTTY ..... 43
5.7.3 General Notes ..... 44
5.7.3.1 SWS MMI Interface ..... 44
5.7.3.2 Supported Ciphers ..... 44
5.8 System Backup and Restoration ..... 44
5.9 SIGTRAN Throughput Licensing ..... 45

**6 Management Interface** ..... 47
6.1 Log On/Off Procedure ..... 47
6.2 Command Entry ..... 47
6.3 Command Responses ..... 48
6.4 Automatic MMI Logging ..... 48
6.5 Parameters ..... 48
6.6 Command Conventions ..... 53
6.7 Commands ..... 53
6.8 Alarm Commands ..... 54
6.8.1 ALLIP – Alarm List Print ..... 54
6.8.2 ALTEE – Alarm Tet End ..... 54
6.8.3 ALTEI – Alarm Test Initiate ..... 55
6.9 Configuration Commands ..... 56
6.9.1 CNBOP – Configuration Board Print ..... 57
6.9.2 CNBUI – Configuration Backup Initiate ..... 57
6.9.3 CNBUS – Configuration Backup Set ..... 57
6.9.4 CNCRP – Configuration MTP Route Print ..... 58
6.9.5 CNCSP – Configuration Concerned Subsystem Print ..... 58
6.9.6 CNGAP – Configuration GTT Address Print ..... 59
6.9.7 CNGLP – Configuration SIGTRAN Gateway List ..... 59
6.9.8 CNGPP – Configuration GTT Pattern Print ..... 60
6.9.9 CNGTP – Configuration Global Title Translation Print ..... 60
6.9.10 CNLSP – Configuration MTP Linkset Print ..... 60
6.9.11 CNMLP – Configuration Monitor Link Print ..... 61
6.9.12 CNOBP – Display TRAP Configuration ..... 61
6.9.13 CNOBS – Set TRAP Configuration ..... 62
6.9.14 CNPCP – Configuration PCM Print ..... 63
6.9.15 CNRDI – Configuration Restore Defaults Initiate ..... 63
6.9.16 CNSLP – Configuration SS7 Link Print ..... 64
6.9.17 CNSMC – Change SNMP Manager Configuration ..... 64
6.9.18 CNSME – End SNMP Manager Configuration ..... 65
6.9.19 CNSMI – Set SNMP Manager Configuration ..... 65
6.9.20 CNSMP – Display SNMP Manager Configuration ..... 66
6.9.21 CNSNP – Configuration SNMP Print ..... 66
6.9.22 CNSNS – Configuration SNMP Set ..... 67
6.9.23 CNSRP – Configuration SIGTRAN Route Print ..... 67
6.9.24 CNSTP – Configuration SIGTRAN Links Print ..... 69

6.9.25 CNSSP – Configuration Subsystem Resource Print ..... 69
6.9.26 CNSWP – Configuration Software Print ..... 70
6.9.27 CNSYP – Configuration System Print ..... 71
6.9.28 CNSYS – Configuration System Set ..... 71
6.9.29 CNTDP – Configuration Time and Date Print ..... 73
6.9.30 CNTDS – Configuration Time and Date Set ..... 73
6.9.31 CNTMP – Configuration Trace Mask Print ..... 74
6.9.32 CNTMS – Configuration Trace Mask Set ..... 74
6.9.33 CNTPE – Configuration Network Time Protocol Server End ..... 76
6.9.34 CNTPI – Configuration Network Time Protocol Server Initiate ..... 76
6.9.35 CNTPP – Configuration Network Time Protocol Print ..... 76
6.9.36 CNUAP – Configuration User Account Print ..... 78
6.9.37 CNUAS – Configuration User Account Set ..... 78
6.9.38 CNUPI – Configuration Update Initiate ..... 79
6.9.39 CNURC – Configuration Update Resource Change ..... 79
6.9.40 CNURE – Configuration Update Resource End ..... 80
6.9.41 CNURI – Configuration Update Resource Initiate ..... 80
6.9.42 CNUSC – Change SNMP v3 User Configuration ..... 81
6.9.43 CNUSE – End SNMP v3 ..... 81
6.9.44 CNUSI – Set SNMP v3 ..... 82
6.9.45 CNUSP – Display SNMP v3 ..... 82
6.10 IP Commands ..... 83
6.10.1 IPEPS – Set Ethernet Port Configuration ..... 83
6.10.2 IPEPP – Display Ethernet Port Configuration ..... 84
6.10.3 IPWSP - Display Web Service Configuration ..... 84
6.10.4 IPWSS -Web Service Configuration Set ..... 85
6.10.5 IPGWI – Internet Protocol Gateway Initiate ..... 85
6.10.6 IPGWE – Internet Protocol Gateway End ..... 86
6.10.7 IPGWP – Internet Protocol Gateway Print ..... 86
6.11 MML Commands ..... 87
6.11.1 MMLOI – MML Log Off Initiate ..... 87
6.11.2 MMHPP – MML Help Print ..... 87
6.12 Maintenance Commands ..... 89
6.12.1 MNINI – Maintenance Inhibit Initiate ..... 89
6.12.2 MNINE – Maintenance Inhibit End ..... 89
6.12.3 MNRSI – Maintenance Restart System Initiate ..... 90
6.13 Measurement Commands ..... 92
6.13.1 MSEPP – Measurement Ethernet Port Print ..... 92
6.13.2 MSHLP – Measurement of Host Links Prints ..... 93
6.13.3 MSLCP – Measurement of License Capability Print ..... 94
6.13.4 MSMLP – Measurement Monitor link Print ..... 95
6.13.5 MSRLP – Measurement Remote Links Print ..... 96
6.13.6 MSPCP – Measurement PCM Print ..... 97
6.13.7 MSSLP – Measurement SS7 Link Print ..... 98
6.13.8 MSSTP – Measurement of SIGTRAN Links Print ..... 99
6.13.9 MSSYP – Measurement System Print ..... 99
6.14 Reset Command ..... 101
6.14.1 RSBOI – Reset Board Initiate ..... 101
6.15 Status Commands ..... 102
6.15.1 STALP – Status Alarm Print ..... 102
6.15.2 STBOP – Status Board Print ..... 103
6.15.3 STCGP – Status Circuit Group Print ..... 103
6.15.4 STCRP – Status SS7 Route Print ..... 104
6.15.5 STDDP – Status Disk Drive Print ..... 105
6.15.6 STEPP – Status Ethernet Port Print ..... 105
6.15.7 STHLP – Status Host Link Print ..... 106
6.15.8 STIPP – Status IP Print ..... 107
6.15.9 STLCP – Status Licensing Print ..... 108
6.15.10 STMLP – Status Monitor Link Print ..... 110
6.15.11 STPCP – Status PCM Print ..... 110
6.15.12 STRAP – Status Remote Application Server Print ..... 111
6.15.13 STRLP – Status Remote SIU Link Print ..... 112
6.15.14 STSLP – Status SS7 Link Print ..... 113
6.15.15 STSRP – Status SIGTRAN Route Print ..... 114
6.15.16 STSSP – Status Sub-System Resource Print ..... 115

6.15.17 STSTP – SIGTRAN Link Status ..... 115
6.15.18 STSYP – Status System Print ..... 116
6.15.19 STTDP – Status TCAP Dialog Print ..... 117
6.15.20 STTPP – Network Time Protocol Status Print ..... 118
6.15.21 STTRP – Status TCAP Resource Print ..... 119
6.16 Network Time Protocol ..... 120
6.17 Command Summary ..... 121

**7 Web-based Management Interface** ..... 123
7.1 Overview ..... 123
7.2 SWS Management ..... 123
7.3 Web-based status and statistics ..... 124

**8 Configuration** ..... 127
8.1 Overview ..... 127
8.1.1 Syntax Conventions ..... 127
8.1.2 Dynamic Configuration ..... 128
8.2 Command Sequence ..... 128
8.3 Detection of Errors in the Configuration File ..... 129
8.4 SIU/SWS Commands ..... 130
8.4.1 SIU_HOSTS – Number of Hosts ..... 130
8.4.2 SIU_REM_ADDR – Other SIU/SWS Ethernet Address ..... 131
8.5 Physical Interface Commands ..... 132
8.5.1 SS7_BOARD – SS7 Board Configuration ..... 132
8.5.2 LIU_CONFIG – Line Interface Configuration ..... 133
8.5.3 STREAM_XCON – Cross Connect Configuration ..... 136
8.6 MTP Commands ..... 138
8.6.1 MTP_CONFIG – Global MTP Configuration ..... 138
8.6.2 MTP_NC_CONFIG – Network Context MTP Configuration ..... 139
8.6.3 MTP_LINKSET – MTP Link Set ..... 141
8.6.4 MTP_LINK – MTP Signaling Link ..... 142
8.6.5 MTP2_TIMER – MTP2 Timer Configuration ..... 144
8.6.6 MTP3_TIMER – MTP3 Timer Configuration ..... 145
8.6.7 MTP_ROUTE – MTP Route ..... 146
8.6.8 MTP_USER_PART – MTP User Part ..... 148
8.6.9 MONITOR_LINK – Monitor Link ..... 149
8.7 SIGTRAN Configuration Commands ..... 151
8.7.1 STN_LAS – SIGTRAN Local Application Server Configuration ..... 151
8.7.2 STN_LBIND – SIGTRAN Local Bind Configuration ..... 152
8.7.3 STN_LINK – SIGTRAN Link Configuration ..... 152
8.7.4 STN_NC – SIGTRAN Network Context ..... 154
8.7.5 STN_RAS – SIGTRAN Remote Application Server Configuration ..... 154
8.7.6 STN_RASLIST – SIGTRAN Remote Application Server List Configuration ..... 155
8.7.7 STN_ROUTE – SIGTRAN Route Configuration ..... 155
8.7.8 STN_RSGLIST – SIGTRAN Route signaling Gateway List Configuration ..... 156
8.8 SCCP Configuration Commands ..... 157
8.8.1 SCCP_CONFIG – SCCP Configuration ..... 157
8.8.2 SCCP_NC_CONFIG – SCCP Network Context Configuration ..... 158
8.8.3 SCCP_GTT – Global Title Translation ..... 158
8.8.4 SCCP_GTT_ADDRESS – Global Title Translation Address ..... 159
8.8.5 SCCP_GTT_PATTERN – Global Title Translation Pattern ..... 161
8.8.6 SCCP_SSR – SCCP Sub-System Resources ..... 162
8.8.6.1 Configuring SCCP Remote Signaling Points ..... 163
8.8.6.2 Configuring SCCP Local Sub-Systems ..... 163
8.8.6.3 Configuring SCCP Remote Sub-Systems ..... 164
8.8.7 SCCP_CONC_SSR – SCCP Concerned Sub-Systems Configuration ..... 165
8.9 TCAP Configuration Commands ..... 166
8.9.1 TCAP_CONFIG – TCAP Configuration ..... 166
8.9.2 TCAP_NC_CONFIG – TCAP Network Context Configuration ..... 167
8.9.3 TCAP_CFG_DGRP – TCAP Dialog Group Configuration ..... 168
8.10 MAP Configuration Commands ..... 168
8.10.1 MAP_CONFIG – MAP Configuration ..... 168
8.10.2 MAP_NC_CONFIG – MAP Configuration ..... 169

8.11 Protocol Configuration Modification ..... 170
8.11.1 Establishing an FTP Session ..... 170
8.11.2 Transferring the Protocol Configuration to a Remote Computer ..... 170

**9 Configuration Guidelines** ..... 171
9.1 Overview ..... 171
9.2 IP Port Bonding ..... 171
9.3 Configuring a Dual Resilient SWS System ..... 171
9.4 Configuring an ANSI System ..... 172
9.5 Specifying Default Routes ..... 172
9.6 Dynamic Host Activation ..... 173
9.7 Dynamic Configuration ..... 173
9.7.1 Config.txt-Based Dynamic Configuration ..... 173
9.8 SIGTRAN M2PA Signaling ..... 175
9.8.1 Overview ..... 175
9.8.2 M2PA License ..... 175
9.8.3 SS7 over M2PA ..... 175
9.8.4 Configuration Examples ..... 175
9.9 SIGTRAN M3UA Signaling ..... 176
9.9.1 Overview ..... 176
9.9.2 Configuration Examples ..... 177
9.9.2.1 SWS to Signaling Gateway ..... 177
9.9.2.2 SWS to Remote Application Server (IPSP Operation) ..... 177
9.10 SIGTRAN M3UA - Dual Operation ..... 178
9.11 GTT Configuration ..... 178
9.11.1 How to configure GTT ..... 178
9.11.2 Global Title Address Information ..... 179
9.11.3 Examples ..... 179
9.11.3.1 Example 1 ..... 179
9.11.3.2 Example 2 ..... 179
9.11.3.3 Example 3 ..... 181
9.11.3.4 Example 4 ..... 181
9.12 HSL Signaling ..... 182
9.12.1 LIU_CONFIG ..... 182
9.12.2 MTP_LINK <interface_mode> ..... 182
9.12.3 MTP_LINK <flags> ..... 182
9.12.4 MTP_LINK <timeslot> ..... 183
9.12.5 MTP_LINK <blink> ..... 183
9.13 ATM Signaling ..... 183

**Glossary** ..... 185

## Figures

1 Overview of SWS mode ..... 9
2 SWS Mode modules supported ..... 12
3 Signaling Paths in a Single SWS Configuration ..... 19
4 Signaling Paths in a Dual Resilient Configuration ..... 20
5 Single SWS Connected to SSP/SCP or STP ..... 20
6 SWS Dual Configuration with Connections to SSP/SCP ..... 21
7 SWS Dual Configuration with Connections to STP ..... 21
8 SWS Dual Configuration with Connections to Mated STP Pair ..... 22
9 Multiple Network Contexts to Support Multiple Local Point Codes ..... 23
10 Multiple Network Contexts with an STP Pair ..... 23
11 Multiple Network Contexts Support for Multiple Network Types ..... 24
12 Module IDs for Use with Multiple Network Contexts ..... 25
13 SWS Management Interface ..... 121
14 SWS Web-based status control panel ..... 122

15 Example status output ..... 123

## Tables

1 Possible Alarm Events ..... 40
2 Command Responses ..... 48
3 Parameter Definitions ..... 48
4 Command Summary ..... 132
5 Supported Actions for Dynamic Configuration ..... 174

## Revision History

| Date | Part Number | Issue No. | Description |
|---|---|---|---|
| November 2010 | 64-1149-01 | 1 | Initial version. |
| January 2011 | 64-1149-02 | 2 | Addtion of MAP Configuration Information and minor corrections to SCCP LSS configuration. |
| April 2011 | 64-1149-03 | 3 | Updates to MMI command syntax. |

***Note:*** The current release of this guide can be found at:
http://www.dialogic.com/support/helpweb/signaling

# Chapter 1: Overview

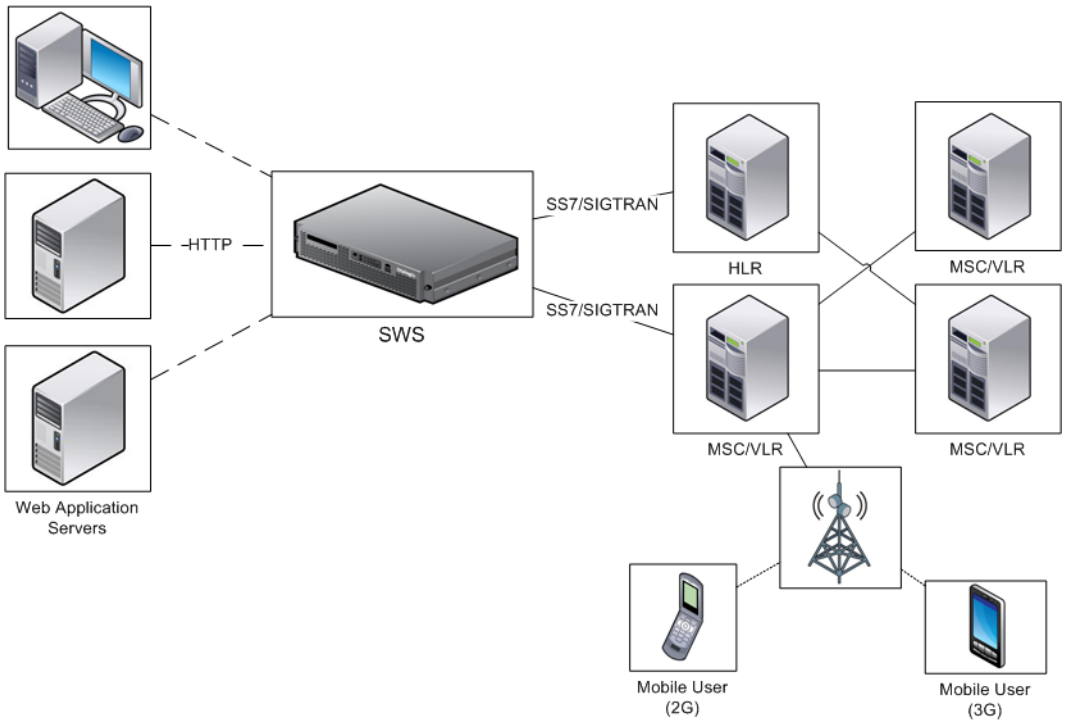
## 1.1 General Description

The Dialogic® DSI Signaling Web Services (SWS) provides an interface to SS7 and SIGTRAN networks for one or more client applications over a Web-Services interface. In this mode, the units implement the SS7 Message Transfer Part (MTP) and a number of User Parts (SCCP, TCAP, MAP). In addition, the SWS implements MAP service functionality and a high-level Application Programming Interface (API) to simplify development for mobile applications such as SMS, USSD and Location Based services.

## 1.2 Key Benefits

- High Level API for mobile network services
  - — Lowers SS7 / GSM MAP protocol knowledge required
  - — Focuses on enabling the most common services to mobile devices
- XML / HTTP Web Service API
  - — Greater choice of development platform and toolsets
  - — Reduced dependency on proprietary interface
- Server based
  - — Based on existing proven server platform

**Figure 1. Overview of SWS mode**




This manual is applicable to the Dialogic® DSI SS7G31 and SS7G32 Signaling Servers.

***Note:*** Throughout this manual, these products are referred to collectively as the Dialogic® DSI Signaling Servers, or as the “Signaling Servers”, or individually, by their particular alphanumeric designation (SS7G31 or SS7G32). In addition, the SS7G31 and SS7G32 models may be referred to collectively as “SS7G3x”. In addition, unless otherwise stated, text within this document is applicable to all servers within the Dialogic® DSI SS7 Signaling Server range when operating in

SWS mode, and the terms “SWS” and “Signaling Web Services” may be used to refer to a Dialogic® DSI Signaling Server being operated in SWS mode.

The Signaling Server may be purchased as one of two equipment types: SS7G31 and SS7G32. Both servers use the same software, but use different chassis and different signaling boards. See Section 1.5, “Hardware Overview” on page 13 for a fuller description of the Signaling Server hardware.

The SS7G31 and SS7G32 Signaling Servers are shipped in TEST Mode - without any operation mode license installed. To enable SWS functionality, order an appropriate SWS license.

### 1.2.1 Other Operating Modes

**Signaling Interface Mode (SIU)**

- A Signaling Server with the SIU Mode software license installed and enabled, operates as a Signaling Interface Unit (hereinafter sometimes referred to as "SIU”), offering SS7 Protocol support over a TCP/IP interface. In this mode the server offers support for many SS7 protocols such as ISUP, BICC, SCCP, TCAP, MAP, INAP and IS41. In addition the server offers support for monitoring applications. Description and use of the system acting as a Siganling Interface Unit is outside the scope of this manual. See the *Dialogic® DSI Signaling Servers SIU Mode User Manual.*

**Signaling Gateway Mode (SGW)**

A Signaling Server with the SGW Mode software license installed and enabled, operates as a SIGTRAN Signaling Gateway (hereinafter sometimes referred to as "Signaling Gateway"), offering support for the M3UA and M2PA SIGTRAN protocols. Description and use of the system acting as a SIGTRAN Signaling Gateway is outside the scope of this manual. See the *SGW Mode User Manual* for a detailed description of this mode of operation.

**Test Mode (TEST)**

Signaling Servers are shipped in Test Mode which allows the system to be activated for operation in one of the other operating modes.

## 1.3 Related Information

Refer to the following for related information:

- *Dialogic® DSI Signaling Servers SWS Application Programmer’s Manual (U01SWD)*
- *Dialogic® DSI Signaling Servers SGW Mode User Manual (05-2304)*
- *Dialogic® SS7 Protocols Software Environment Programmer’s Manual (U10SSS)*
- *Dialogic® DSI Signaling Servers SNMP User Manual (U05EPP)*
- *Dialogic® DSI Signaling Servers User Manual Supplement for ATM Operation (U01LFD)*
- *Dialogic® DSI Signaling Servers SIU Mode User Manual (05-2302)*

The current software and documentation supporting Dialogic® DSI Signaling Server products is available on the web at:http://www.dialogic.com/support/helpweb/signaling/.

The product data sheet is available at:http://www.dialogic.com/support/helpweb/signaling/.

For more information about Dialogic® SS7 products and solutions, visit:http://www.dialogic.com/support/helpweb/signaling/.

The following manuals should be read depending on the protocol options installed on the SWS:

- *SCCP Programmer’s Manual (U05SSS)*
- *TCAP Programmer’s Manual (U06SSS)*
- *MAP Programmer’s Manual (U14SSS)*
- *SCTP Programmer’s Manual (U01STN)*
- *M3UA Programmer’s Manual (U02STN)*
- *M2PA Programmer’s Manual (U03STN)*

## 1.4 Applicability

This manual is applicable to SS7G31 and SS7G32 operating in SWS Mode Release 1.0.0 mode only.

This manual is not applicable if operating in other modes such as SIGTRAN Signaling Gateway (SGW) or Signaling Interface Unit (SIU).

## 1.5 Hardware Overview

The Signaling Server may be purchased as one of the following equipment types:

- An SS7G31 is a 1U Signaling Server and may be purchased with one Dialogic® DSI SPCI4 Network Interface Board, (with 4 SS7 links and 4 T1/E1 interfaces), or one Dialogic® DSI SS7HDP Network Interface Board, (with 64 SS7 links and 4 T1/E1 interfaces or 2 HSL links).
- An SS7G32 is a 2U Signaling Server and may be purchased with one, two or three Dialogic® DSI SS7HDP Network Interface Boards (with 64 links and 4 T1/E1 interfaces per board or 2 HSL links per board) with a system maximum of 192 LSL SS7 links or 6 HSL SS7 links.

***Note:*** The SS7G32 also supports the installation in the field of up to 2 Dialogic® SS7MD Network Interface Boards. These SS7MD boards may be used for termination and monitoring of ATM signaling links. SS7MD boards cannot be installed in an SS7G31 or SS7G2x Signaling Server. When using two SS7MD boards, the maximum link density for the SS7G32 is increased to 248 low speed or 8 high speed signaling links, which can be either ATM or Q.703 Annex A. See the Signaling Servers User Manual Supplement for ATM Operation for further information regarding the installation and operation of SS7MD signaling boards.

When T1 or E1 is selected, the Signaling Server may be configured to pass the bearer channels from one PCM port to another, effectively “dropping out” the signaling in line.

The SS7G31 and SS7G32 support two hard disks configured as a RAID 1 array.

See Chapter 2, “Specification” for a definition of the capabilities of the system.

### 1.5.1 Part Numbers

For the SS7G31 and SS7G32 products, refer to the *Dialogic® DSI SS7G31 and SS7G32 Signaling Servers Product Data Sheet* (navigate from http://www.dialogic.com/products/signalingip_ss7components/signaling_servers_and_gateways.htm) for a list of the ordering codes and definitions of the hardware variants of the two equipment types.

## 1.6 Signaling Overview

The signaling capability of the SWS depends on the number and type of signaling boards installed. Up to a maximum of 64 link sets and 504 signaling links are supported.

All link sets terminate at an adjacent signaling point, which may be a Signaling Transfer Point (STP), allowing the use of the quasi-associated signaling mode. When operating as a pair, resilience is provided at MTP3 through the use of a link set between the two units.

In addition to SS7 over TDM signaling, the SWS supports the SIGTRAN M2PA and M3UA protocols. A maximum 256 M2PA or M3UA links are configurable - depending on the license installed.

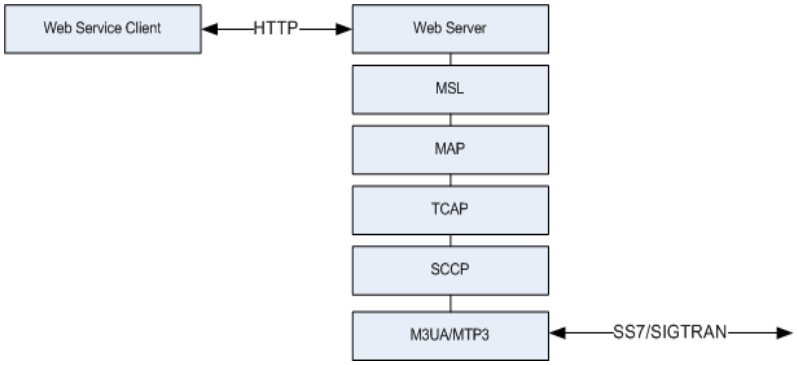
The SWS will also allow mixed configurations deploying SS7 over TDM, SS7 over ATM, SS7 over M2PA and SS7 over M3UA signaling. Resilience can be achieved using M2PA or M3UA links between a pair of units.

## 1.7 Functional Summary

### 1.7.1 SWS Mode Overview

The Signaling Server, when operating in SWS Mode, provides a web-services interface at the top and supports all of the SS7 modules required beneith down to the SS7 links or SIGTRAN associations.

**Figure 2. SWS Mode modules supported**




### 1.7.2 Application Software

Application Development and the API used for this are covered in detail in the Dialogic® DSI Signaling Servers SWS Application Programmer's Manual.

Examples of application modules are supplied in source code form for use on the client host computer.

### 1.7.3 Fault Monitoring

The SWS is able to detect internal fault conditions and report these to the user. The internal faults are combined with external events, to provide an alarm reporting function, which has several possible interfaces to the user, and may be local or remote. For further information on alarm functions refer to Section 3.8, "Alarms" on page 29.

#### 1.7.3.1 Diagnostic Log Files

The SWS is able to generate several diagnostic log files for use in the event of an unexpected system restart. The text files can be recovered from the unit using FTP.

### 1.7.4 Management Interface

A management interface is provided and may be accessed either via a VT100-compatible terminal or remotely via telnet or SSH. This is used to request information on the status of signaling links and PCM ports. The management interface also provides configuration information and activation of tracing. In addition a some aspects of the system maybe set up using a web-based configuration interface.

### 1.7.5 IP Security

The SWS offers a number of security features for protection against unwarranted access on its IP interface. It is recommended that the user enables the optional Password Protection feature on the Management Interface port and on the FTP Server port.

For additional security, the SWS is equipped with Secure Shell (SSH) functionality, which supports the tunneling of **telnet** and **RSI** traffic, as well as Secure FTP.

Unused ports are disabled to increase security against unintentional or malicious interference.

Additional security may be gained by separating management and signaling IP traffic. This can be achieved by configuring specific Ethernet ports for traffic and utilizing other Ethernet ports for system management information. Signaling IP traffic security between the SWS and its hosts can be further enhanced by tunneling the IP traffic over SSH.

It should be understood that while the SWS has been designed with security in mind, it is recommended that the SWS accessibility over IP be restricted to as small a network as possible. If the unit is accessible by third parties, then the use of a third-party firewall should be considered.

# Chapter 2: Specification

## 2.1 Hardware Specification

Hardware details of the Signaling Server products are provided in the *Dialogic*® DSI SS7G31 and SS7G32 Signaling Servers Hardware Manual.

The Dialogic® DSI SS7G31 and SS7G32 Signaling Servers physically identify Ethernet ports in different ways. Below is a mapping between the Ethernet port as it is identified in software and the physical port as it is identified in the respective Hardware Manual:

- SS7G31: Ethernet ports number in the range 1 to 4, where:
  - ETH=1 corresponds to physical port 1
  - ETH=2 corresponds to physical port 2
  - ETH=3 corresponds to physical port 3
  - ETH=4 corresponds to physical port 4
- SS7G32: Ethernet ports number in the range 1 to 6, where:
  - ETH=1 corresponds to physical port 1
  - ETH=2 corresponds to physical port 2
  - ETH=3 corresponds to physical port ACT/LNK A (bottom)
  - ETH=4 corresponds to physical port ACT/LNK B (bottom)
  - ETH=5 corresponds to physical port ACT/LNK A (top)
  - ETH=6 corresponds to physical port ACT/LNK B (top)

## 2.2 Software Licenses

This section identifies which licensable capabilities can be purchased for Signaling Server SWS Mode operation.

For information relating to the purchase, installation and activation of software licenses, see Chapter 4, “Licensing, Installation and Initial Configuration”.

### 2.2.1 Software Licenses for SS7G31 and SS7G32

The following SS7G30 licenses can be purchased for SWS mode:

| ITEM MARKET NAME | DESCRIPTION |
|---|---|
| SS7SBG30SWS4 | Signaling Web Services, 4 MTP3 links, Messageing, Location Services |
| SS7SBG30SWS8 | Signaling Web Services, 8 MTP3 links, Messaging, Location Services |
| SS7SBG30SWS16 | Signaling Web Services, 16 MTP3 links, Messaging, Location Services |
| SS7SBG30SWS32 | Signaling Web Services, 32 MTP3 links, Messaging, Location Services |
| SS7SBG30SWS64 | Signaling Web Services, 64 MTP3 links, Messaging, Location Services |
| SS7SBG30SWS128 | Signaling Web Services, 128 MTP3 links, Messaging, Location Services |
| SS7SBG30SWS256 | Signaling Web Services, 256 MTP3 links, Messaging, Location Services |
| SS7SBG30M3UAS | M3UA supporting 16 SIGTRAN links and up to 154 Kilobytes/sec, equivalent to 16 Low speed TDM links at 0.6 Erlangs |
| SS7SBG30M3UAR | M3UA supporting 32 SIGTRAN links and up to 308 Kilobytes/sec, equivalent to 32 Low speed TDM links at 0.6 Erlangs |
| SS7SBG30M3UAL | M3UA supporting 64 SIGTRAN links and up to 615 Kilobytes/sec, equivalent to 64 Low speed TDM links at 0.6 Erlangs |
| SS7SBG30M3UAK | M3UA supporting 128 SIGTRAN links and up to 1230Kilobytes/sec, equivalent to 128 Low speed TDM links at 0.6 Erlangs |

| ITEM MARKET NAME | DESCRIPTION |
|---|---|
| SS7SBG30M3UAJ | M3UA supporting 256 SIGTRAN links and up to 2460 Kilobytes/sec equivalent to 256 Low speed TDM links at 0.6 Erlangs |
| SS7SBG30M2PAS | M2PA supporting 16 SIGTRAN links and up to 154 Kilobytes/sec equivalent to 16 Low speed TDM links at 0.6 Erlangs |
| SS7SBG30M2PAR | M2PA supporting 32 SIGTRAN links and up to 308 Kilobytes/sec equivalent to 32 Low speed TDM links at 0.6 Erlangs |
| SS7SBG30M2PAL | M2PA supporting 64 SIGTRAN links and up to 615 Kilobytes/sec equivalent to 64 Low speed TDM links at 0.6 Erlangs |
| SS7SBG30M2PAK | M2PA supporting 128 SIGTRAN links and up to 1230 Kilobytes/sec equivalent to 64 Low speed TDM links at 0.6 Erlangs |
| SS7SBG30M2PAJ | M2PA supporting 256 SIGTRAN links and up to 2460 Kilobytes/sec equivalent to 256 Low speed TDM links at 0.6 Erlangs |

All of the above licenses offer the same basic functionality but vary in the number of MTP3 links supported. The M3UA or M2PA licenses are required in order to support SIGTRAN operation and offer different levels of link-equivilent throughput.

## 2.3 Capabilities

This section identifies notable capabilities of the Signaling Server. The capabilities of a Signaling Server is dependent on the number and type of signaling boards installed as defined by the product variant as well as which software licenses installed.

Use of Signaling Servers in dual pairs increases the capacity of the overall system while still acting as a single SS7 point code. The numbers given in this section are for a single Signaling Server.

### 2.3.1 SS7G31 and SS7G32 Signaling Servers Protocol Capabilities

| Feature or Protocol | SS7G31 Capabilities | SS7G32 Capabilities |
|---|---|---|
| Dialogic® DSI SS7 Network Interface Boards | Up to 1 SPCI4 board or 1 SS7HDP board | Up to 3 SS7DHP boards, up to 3 SPCI4 boards, or up to 2 SS7MD boards |
| Portable Media Device | USB | USB |
| PCM per board | 4 per SPCI4 or 4 per SS7HDP | 4 per SPCI4, 4 per SS7HDP or 4 per SS7MD |
| Ethernet interface | 4 | 6 |
| SS7 links per board | 4 per SPCI4 or 64 per SS7HDP | 4 per SPCI4, 64 per SS7HDP or 124 per SS7MD |
| HSL links per board | 2 per SS7HDP | 2 per SS7HDP |
| ATM links per board | | 4 per SS7MD |
| M3UA links | 256 | 256 |
| M2PA links | 256 | 256 |
| SS7 linksets | 64 | 64 |
| SS7 links | 64 | 248 |
| SS7 routes | 4096 | 4096 |
| Remote Application servers | 256 | 256 |
| M3UA routes | 256 | 256 |
| Network contexts | 4 | 4 |
| SCCP | Up to 512 Local sub-systems, remote sub-systems, or remote signaling points. | Up to 512 Local sub-systems, remote subsystems, or remote signaling points. |
| TCAP | Up to 65,535 simultaneous active dialogs | Up to 65,535 simultaneous active dialogs |
| MAP | Up to 65,535 simultaneous active dialogs | Up to 65,535 simultaneous active dialogs |
| Hosts | Up to 128 hosts | Up to 128 hosts |

### 2.3.2 Application Interfaces

Supports RESTful HTTP interface

| Feature or Protocol | Capabilities |
|---|---|
| Inteface Architectural Style | RESTful |
| Payload | XML |
| XSD schema provided | yes |

# Chapter 3: Architecture

## 3.1 Overview

The Dialogic® DSI Signaling Server for Signaling Web Services (SWS) allows client applications to offer services which make use of SMS, USSD and location functionality. The SWS unit connects into SS7 or SIGTRAN networks and provides APIs to allow one or more instance of a client application to control this functionality. The SS7 configuration parameters are specified in a text file contained within each SWS. This is described in Chapter 8, “Configuration”.

A complete system requires, in addition to the SWS unit, at least one active client application. The client applications communicate with the SWS using a web-service interface. For a description of the client applicator development APIs, please refer to the Dialogic DSI Signaling Servers SWS Application Programmer’s Manual.

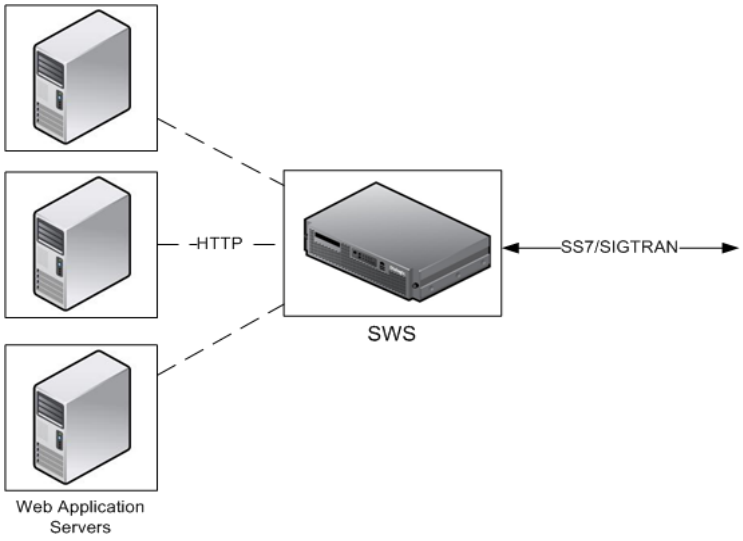
## 3.2 Signaling Topologies

A single SWS may be used standalone, or two units may be configured in a dual resilient configuration. Each SWS may support one or more application (host) computers.

The host computer contains the physical resources controlled by the signaling, such as voice circuits and databases. The SWS extracts SS7 information and conveys it to the application software, which can control the resource accordingly and issue the required responses to the SWS for transport over the SS7 network.

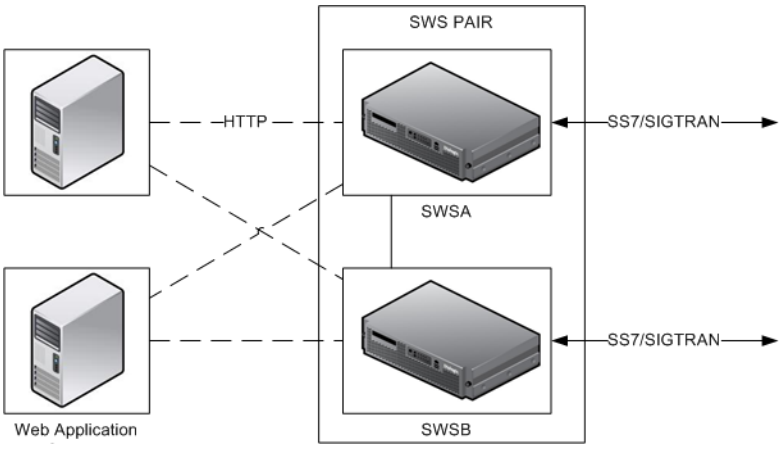
The minimal system consists of a single SWS connected to a single host via Ethernet as illustrated in Figure 3. Dashed lines indicate optional equipment.

**Figure 3. Signaling Paths in a Single SWS Configuration**




This system may be scaled up at initial system build time or later to a dual resilient configuration connected to the maximum number of hosts supported. See Figure 4.

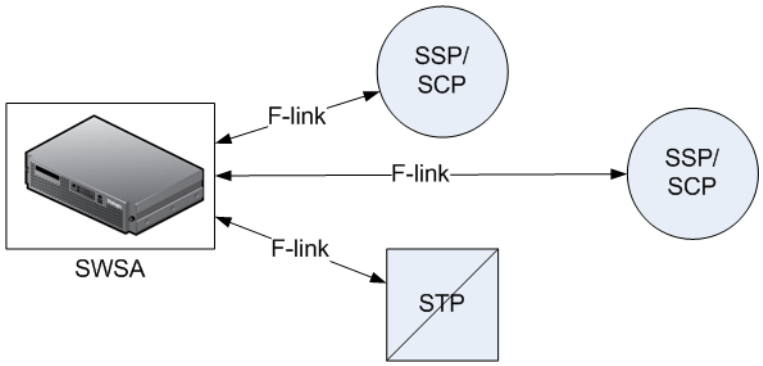
**Figure 4. Signaling Paths in a Dual Resilient Configuration**




The SWS may connect to a number of adjacent signaling points, the maximum number being limited only by the maximum number of link sets supported by the unit. The adjacent SS7 nodes may be Signaling Transfer Points (STPs), Signaling Switching Points (SSPs) or Signaling Control Points (SCPs). The following diagrams indicate possible configurations, although these are not exhaustive.

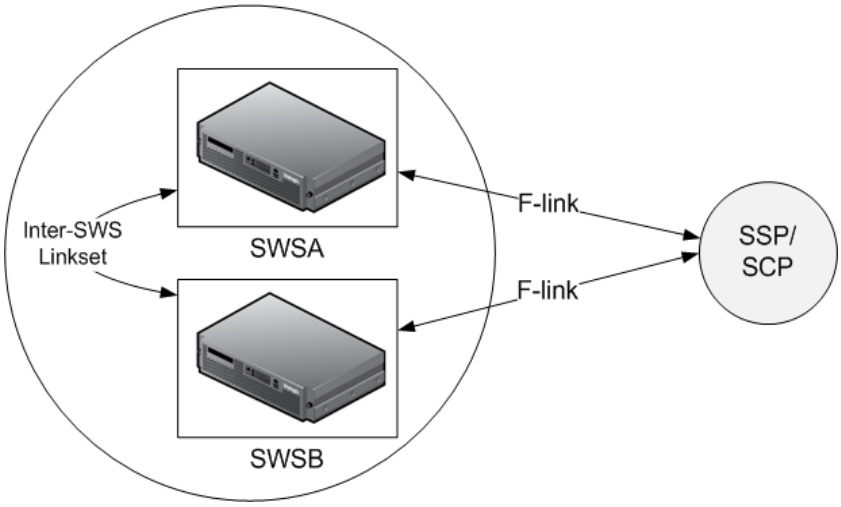
Figure 5 shows a single SWS connected to an adjacent SSP/SCP and/or STP.

**Figure 5. Single SWS Connected to SSP/SCP or STP**



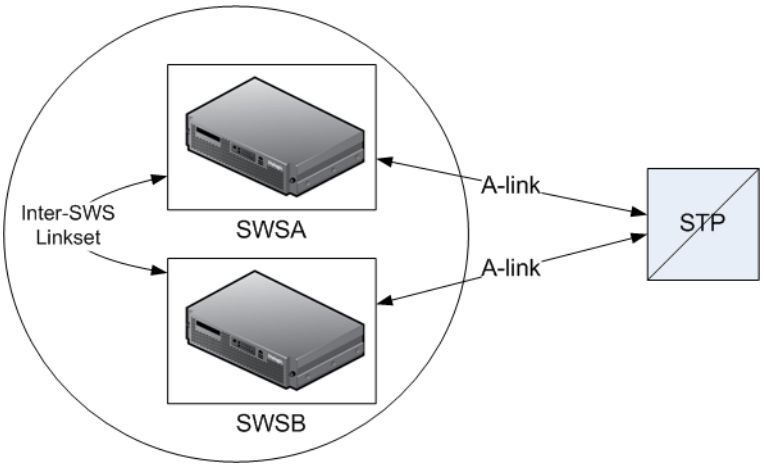

In a dual resilient configuration, the SWS pair *share the same SS7 point code*. Figure 6 shows an SWS pair connected to a single adjacent SSP/SCP.

**Figure 6. SWS Dual Configuration with Connections to SSP / SCP**



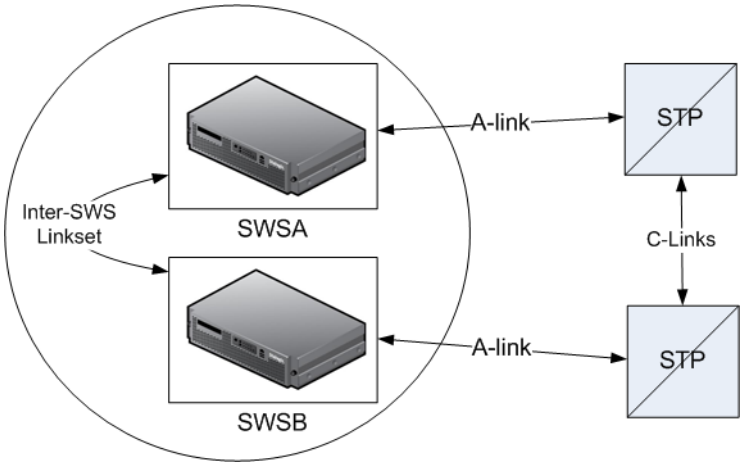

The SWS pair may also be connected to a single adjacent STP (or combination of SSP and STP) as shown in Figure 7.

**Figure 7. SWS Dual Configuration with Connections to STP**




Finally, Figure 8 shows an SWS pair connected to a “mated” STP pair. In this configuration, all the links from the first STP must be terminated at SWSA and all the links from the second STP must be terminated at SWSB.

**Figure 8. SWS Dual Configuration with Connections to Mated STP Pair**




## 3.3 Multiple Network Support

The SS7 Network Context, together with a signaling point code, uniquely identifies an SS7 node by indicating the specific SS7 network to which it belongs. The Network Context may be a unique identifier for a physical SS7 network, for example, to identify an ANSI, ITU, International or National network, or it may be used to subdivide a physical SS7 network into logical sub-networks. An example of the use of logical networks is in provisioning, where the user requires 64 SS7 links between two point codes in a network. As the SWS supports 16 links in a link set, and one link set between two points in a network, only 16 links between two points would normally be achievable. However, if the network is divided into four logical Network Contexts, then up to four link sets may be created between the two point codes, one in each Network Context, thus allowing up to 64 SS7 links to be configured between the two points.

***Note:*** The Network Context has significance only to the configuration of the local node (including the hosts). No external messages include any indication of the Network Context and the configuration of remote systems is unaffected.

The SWS mode is able to support architectures in which a single SWS or dual resilient SWS pair are connected into one or more different SS7 networks. The SWS or SWS pair can also independently terminate multiple local point codes within the same network. Section 3.3.1 and Section 3.3.2 following describe these different architectures.

The SWS can support up to four Network Contexts, where each Network Context is a different network or different independent local point code within the same network. In the configuration commands or MMI commands, Network Contexts are designated NC0, NC1, NC2 or NC3. Network Context NC0 is also referred to as the default Network Context since this is the Network Context that is assumed if no other explicit value is specified within the command.

### 3.3.1 Support for Multiple Local Point Codes

In some situations, it is desirable to have an SWS terminate more than one local point code within the same SS7 network. Each local point code can have separate routes and associated pairs of link sets to a destination point code. This means that adding additional local point codes allows additional link sets to be used to send traffic to a destination point code. As link sets are limited to 16 links, adding more link sets using multiple local point codes effectively allows a larger total number of links to carry traffic to any single destination point code.

Figure 9 shows a simple configuration that uses two Network Contexts to allow a single SWS to connect to the remote node using two link sets from two independent local point codes. Link set 0 and 1 are configured in Network Contexts NC0 and NC1 respectively.

**Figure 9. Multiple Network Contexts to Support Multiple Local Point Codes**

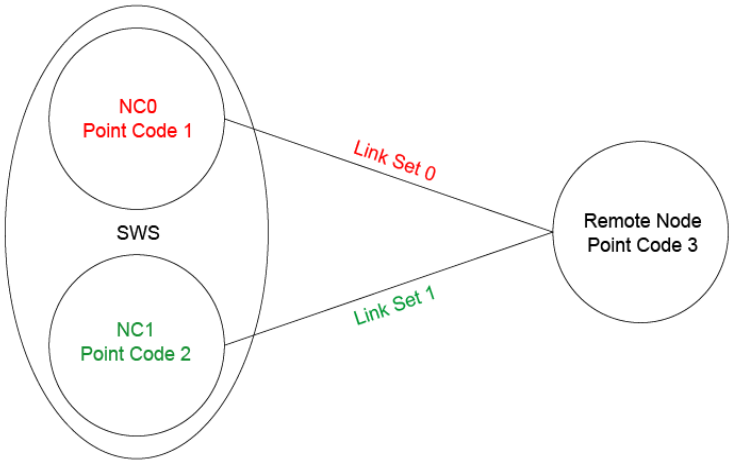
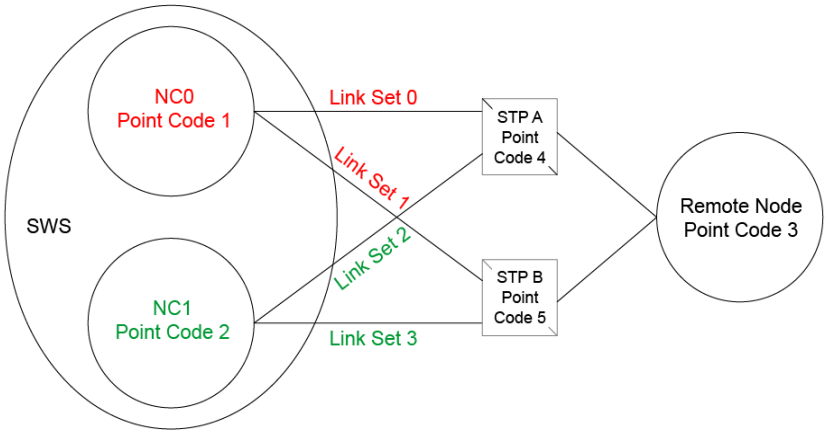



Figure 10 extends the previous example to show a configuration with an STP pair. This configuration uses two Network Contexts to allow a single SWS to connect to the Remote Node using four link sets from two independent local point codes. An equivalent configuration using a dual resilient pair is also possible.

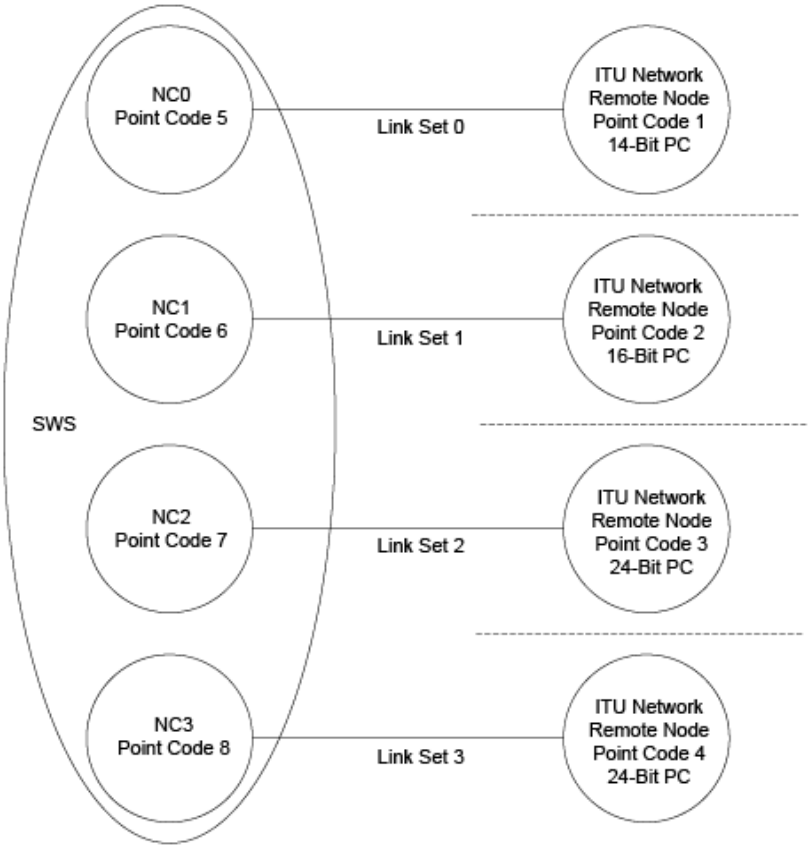
**Figure 10. Multiple Network Contexts with an STP Pair**



### 3.3.2 Support for Multiple Networks

The Network Context-based configuration of the SWS mode allows the settings and behavior to be configured independently for each Network Context. This allows a system to be configured with mixed ITU and ANSI network types or allows multiple networks of the same type to be configured with different settings.

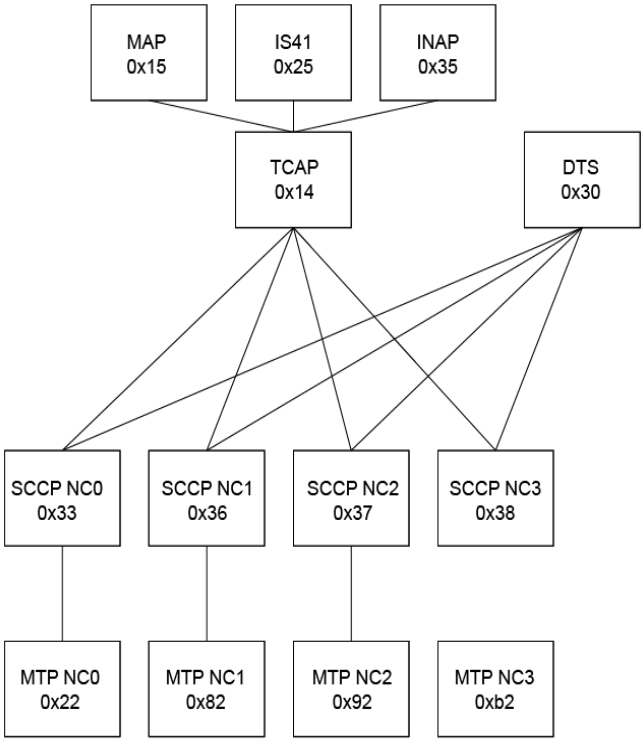
**Figure 11. Multiple Network Contexts Support for Multiple Network Types**



### 3.3.3 Protocol Handling for Multiple Network Contexts

Figure 12 shows the use of multiple Network Contexts from an application perspective and provides examples of the module IDs for the various application layers.

**Figure 12. Module IDs for Use with Multiple Network Contexts**




#### 3.3.3.1 MTP Applications

Since there is one instance of MTP3 for each Network Context, messages that are destined for a specific network must be sent to the correct MTP module ID as shown in Figure 12 above.

In most SWS configurations, MTP is not the highest protocol layer and the sending of messages to the correct module is handled by the higher layer modules without further user interaction.

#### 3.3.3.2 SCCP Applications

In the same manner as MTP3, there is one instance of SCCP for each Network Context; therefore, messages that are destined for a specific network must be sent to the correct SCCP module ID as shown in Figure 12.

When TCAP or DTS is used above SCCP, those modules handle the sending of messages to the correct module without further user interaction.

#### 3.3.3.3 TCAP/MAP Applications

Where a dialog is initiated remotely, no change is required since TCAP and MAP automatically determine which Network Context is appropriate. Where the dialog is initiated locally, the application must specify the Network Context to which the message is destined. This effectively indicates the point code to be used as the originating point code.

The Network Context should be indicated in the first message for the dialog being used. In the case of TCAP, this is in the first TCAP service request, typically an Invoke Req, using the TCPPN_NC parameter. For MAP, the Network Context should be indicated in the Open Request message, instead of using the MAPPN_NC parameter.

If a Network Context is not specified, the default Network Context, NC0 is assumed.

## 3.4 Inter-SWS Communication

In a dual resilient configuration (one unit nominated as SWSA, the other as SWSB), two physically independent communication channels exist between the two units.

Control information is exchanged over the Ethernet. Signaling messages are exchanged (when necessary) over an inter-SWS SS7 link set, *which must be configured for correct dual resilient operation.*

The preferred route for messages transmitted from an SWS is over the links connecting that unit to the appropriate adjacent point code (a point code that is either the final destination or a route to the final destination). If no signaling link to an appropriate adjacent point code is available, the transmit traffic is passed to the other SWS via the inter-SWS link set. If the inter-SWS link set fails, transmit messages fall back to being passed over the Ethernet.

If the inter-SWS link set fails (causing the Ethernet link to be used for transmitted messages), message loss may occur at the point where the preferred route fails.

The SS7 network is free to deliver received messages to either SWS. Special processing at the User Part level provides that any message received for a call or transaction being handled by the other unit is routed over the Ethernet.

The inter-SWS link set is configured in the same manner as normal link sets, for details, refer to Chapter 8, “Configuration”.

The inter-SWS link set may consist of one or more signaling links configured between the dual resilient pair. Resilience on the Inter SWS link set may be achieved by configuring two links in the inter-SWS link. The inter-SWS link may be conveyed over M2PA or M3UA avoiding the requirement for a TDM link and cabling between the units or may be conveyed via signaling links configured on the T1/E1 ports.

## 3.5 Transaction-Based Applications

Applications that need to exchange non-circuit related information over the SS7 network (such as for the control of a Mobile Telephone Network or for an Intelligent Network application) do so by exchanging information between *sub-systems* using the services of SCCP. A sub-system is an entity that exchanges data with other entities by using SCCP.

The SWS provides the capability to configure local sub-systems and routing to remote resources. The intelligent functionality of each local sub-system is provided by the user application running on one or more host computers.

### 3.5.1 Management of Local SCCP Sub-Systems

The SWS system automatically brings local SCCP sub-systems into service; no application interaction is required.

## 3.6 Resilience

### 3.6.1 IP Resilience

The SWS has up to six IP ports. These ports may be configured with IP addresses in separate IP networks to allow greater IP resilience on the SWS. IP addresses are configured using the IPEPS command. The IPGWI command allows configuration of the default gateway and additional gateways.

As the SWS supports static, rather than dynamic IP routing, the SWS should not be configured with different IP addresses within the same IP network. Instead, resilience between two IP ports within the same network can be achieved by using IP port bonding, which allows two physical IP ports to be bonded together in an active/standby configuration under a single IP address. See Section 9.2, “IP Port Bonding” on page 171 for more information.

## 3.7 Management Reporting

The SWS reports management alarms such as PCM trunk status and SS7 level 2 link status to a single software process, identified as module_id **0xef**, that exists by default on host 0. The user management application is responsible for interpreting the management messages (described in Chapter 10, “Application Programming Interface”), performing the appropriate action and distributing these messages to other hosts if required. The identity of the default management host is displayed by the DMHOST parameter on the CNSYP MMI command and may be changed through use of the CNSYS command.

Any host may assume the role of management by sending a management request (in the form of an API_MSG_COMMAND request). On receipt of this request, the SWS begins to send management events to the new host. Unlike the setting of the DMHOST through MMI setting of a management host, using the API_MSG_COMMAND will require the user to transmit the API_MSG_COMMAND with the desired management host identify each time the SWS is restarted.

An optional second management host may also be activated by sending a management request. On receipt of this request, the SWS sends management events to both management hosts.

The selection of which host is the manager, as well as the configuration of an additional management host, allows a user to build a resilient solution to meet their management event reporting needs.

The SWS also maintains a log of management messages for diagnostic purposes in the "syslog" subdirectory of the siuftp account. This log is maintained as a rolling log of up to 10 5MB files containing management messages transmitted to the management host as well as some further diagnostic data. The most recent maintenance log file will have the name “maint.log” the next most recent “maint.log.1” and then “maint.log.2” and so on.

## 3.8 Alarms

The Dialogic® DSI Signaling Server products are able to detect a number of events or alarm conditions relating to either the hardware or the operation of the protocols. Each alarm condition is assigned a severity/ class (3=Critical, 4=Major, 5=Minor) and a category and ID, which give more detail about the alarm. There are a number of mechanisms described below, by which these conditions can be communicated to management systems, and ultimately to the system operator. See Section 5.5, “Alarm Listing” on page 40 to for a list of alarm types, and their reporting parameters.

- Active alarms are indicated on the front panel of the Signaling Server (except SS7G31), with three LEDs identifying severity; CRT, MJR, MNR.
- Active alarms may be indicated remotely from the Signaling Server (except SS7G31), when the alarm relay outputs are connected to a remote management system.
- Alarm events (occurrence and clearing, class, category and ID) may be reported via Management messages to the host application as detailed in Chapter 10, “API Commands”, thus permitting remote monitoring and/or logging.
- Alarm events may be reported to an SNMP manager. SNMP support is described in Section 5.4, “SNMP” on page 39.
- A system operator can obtain a listing of the current alarm status (CLA, CATEGORY, ID and TITLE) using the ALLIP management terminal command described in Section 6.8.1, “ALLIP” on page 54. Test Critical,

Major, or Minor may be activated using the ALTEI management command and cleared using the ALTEE management command.

# Chapter 4: Licensing, Installation and Initial Configuration

## 4.1 Software Licensing

Functional capabilities and signaling protocols are activated on the Signaling Server through the use of software licenses. The following section provides information on the purchase of software licenses as well as information relating to temporary operation of the Signaling Server without software licenses.

Software licenses supported on the Signaling Server for SWS mode are identified in Section 2.2, “Software Licenses” on page 17.

### 4.1.1 Purchasing Software Licenses

1. Place an order using your normal sales channel, quoting the product ID for the software option required.

   At this point in the process, there is no need to know details of the specific Signaling Server on which the option is to be installed (the target Signaling Server).

   The order ships through the normal supply channels and you will receive a paper License Certificate. The certificate contains the license terms for using the Signaling Server software option and a unique License ID that is needed to activate the license.

2. When the License Certificate is received, you should first read the full terms of the software license:

   — If you do not agree with the software license terms, contact your sales channel for a refund. You must not activate the software license.

   — If you agree the software license terms, you can continue with Step 3..

3. The next stage is to identify the Dialogic® DSI Signaling Server product(s) on which the software option is to be activated. To do this, you need to obtain the UNIT ID for the Signaling Server which is done by executing the CNSYP MML command (see Section 6.9.27 on page 71) on the target Signaling Server.

4. Once you have the License ID and the UNIT ID, the license can be activated on the Signaling Server. License Activation is the process of submitting the License ID and UNIT ID so that a License File can be generated and sent for installation on the target Signaling Server.

   The License Activation process is web-based, and the License File is sent by email. To activate the license perform the following steps:

   a. Visit the web site: http://membersresource.dialogic.com/ss7/license/license.asp (or an alternative URL if listed on the License Certificate).

   b. Provide the following information:

      — Name

      — Company

      — Country

      — Email address (this will be used to send the License File)

   c. Provide the following information about the Signaling Server:

      — Operating System - Enter "Signaling Server".

      — Host ID - Enter the UNIT ID.

      — User machine identification - A string, typically the SWS name, used by you to identify the unit. This may be any value relevant to you, for example, "SWS_TEST_UNIT1".

   d. Provide the License ID (taken from the License Certificates) for each protocol that is to be licensed on the target Signaling Server.

   e. Submit the form. You will receive confirmation that your request has been submitted. Subsequently, you will receive your License File by email.

### 4.1.2 Temporary Licenses

A temporary software license can be issued for a spare or backup signaling server in the event that an existing server encounters a problem that requires the unit to be repaired or replaced. Alternatively, a new permanent license, based on the licenses from the failed unit, can be issued for a spare signaling server.

The process for obtaining a temporary license file is almost identical to that of activating a new license. On the web based activation form, the License IDs should be prefixed with the following 4 characters: BAK-. For example, if the license ID on the certificate is G30-M3UAS-785-9187, the license ID specified on the web form for the corresponding temporary license would be BAK-G30-M3UAS-785-9187. The Host ID entered on the form is that of the replacement system on which the license will be installed. A temporary license file will then be sent to the email address you specify during the license activation.

A temporary license will allow operation of a spare/backup unit for a period of 30 days from date of issue, after which the system software cannot be restarted. It is therefore important to seek authorization to re-activate the original license(s), to perform the new activation, and to install the new license file prior to the expiry of the 30 day period.

### 4.1.3 Trial Licenses

When the trial license is active, SWS protocols are available on the unit for one hour. After this period, the system will automatically re-boot and return to normal operation supporting only the capabilities that are licensed on the system. To activate trial mode, the unit should be restarted as follows:

```
MNRSI:RESTART=TRIAL;
```

A new “Trial mode” alarm, will be active whenever the system is operating in this mode.

## 4.2 Installing the SWS Unit

***Caution:*** The SWS should only be installed by suitably qualified service personnel. Important safety and technical details required for installation are given in the appropriate system hardware manual.

In order to complete the installation of the SWS unit, proceed as follows:

1. Connect a VT100 terminal to the unit (see Section 4.2.1).
2. Set the IP addresses of the unit (see Section 4.2.2).
3. Check whether a software download and upgrade is required (see Section 4.2.3).
4. Install any additional protocol software option licenses that you may have purchased. (see Section 4.2.4).
5. Check that the system is operating in SWS mode. This is achieved by connecting a VT100 terminal and issuing the CNSYP command. The resulting output shows the operating mode, which is either “SWS“, “SIU” or “SGW” (see Section 6.9.27, “CNSYP” on page 71).

   If the operating mode is not “SWS” and needs to be reset to “SWS” mode, this can be achieved by restarting the software with the following MNRSI command:

   ```
   MNRSI:SYSTYPE=SWS,RESTART=SOFT;
   ```

6. Apply the configuration to the unit (see Section 4.2.5, “Configuration Procedure” on page 35). See also Chapter 9, “Configuration Guidelines” for some example configurations.
7. The SWS is designed to work in a complete system with one or more host platforms. Typical system topologies are shown in Section 3.2, “Signaling Topologies” on page 21.

### 4.2.1 Connecting a VT100 Terminal

A VT100 compatible terminal can be connected, using a DKL29 cable, to the serial port (COM2) on the rear of the unit. After pressing the carriage return (Enter) key, the Signaling Gateway interface prompt is displayed. Default serial port settings are 9600 baud, 8 data bits, 1 stop bits and no parity bits.

The output on the VT100 screen is similar to one of the following:

```
SS7G30(SWS) logged on at 2004-01-20 14:52:29
```

```
<
```

to indicate SWS operation,

OR

```
SS7G30(SIU) logged on at 2004-01-20 14:52:29
<
```

to indicate SIU operation,

### 4.2.2 IP Configuration

The SWS should be connected to the Ethernet network using an RJ-45 (10/100/1000 BASE-T) cable.

The SWS is configured with a default IP address of 192.168.0.1. If this address is not unique, or not suitable for the existing network configuration, it will be necessary to change this value to a unique IP address in the Ethernet network to which it is connected. Instructions for making this change are provided in the following paragraphs.

A VT100 compatible terminal should be connected, using a DKL29 cable, to the serial port (COM 2) on the rear of the unit. After pressing the carriage return, ENTER key, the SWS interface prompt is displayed. The default serial port settings are: 9600 Baud, 8 data bits, 1 stop bits and no parity bits.

```
SS7G30(SWS) logged on at 2004-09-01 00:28:13
<
```

The IP address is set by entering the IPEPS system configuration command, described in Chapter 6, “Management Interface”. For example, to set the IP address to 123.124.125.126, enter the following command:

```
ipeps:eth=1,ipaddr=123.124.125.126;
```

It is also possible to configure a sub-net mask if the unit is a member of a sub-net. The default sub-net mask is 255.255.255.0. To set the sub-net mask to a different value, enter a command similar to the following (where in this example, the sub-net mask is set to 255.255.255.192):

```
ipeps:eth=1,subnet=255.255.255.192;
```

The management interface also allows an IP gateway address to be specified using the GATEWAY parameter in the IPGWx command. By default, this is set to 0.0.0.0, indicating that no gateway is present. To set the gateway address to 123.124.125.250 for example, the following command is used:

```
IPGWI:IPGW=DEFAULT,GATEWAY=123.124.124.250;
```

The current settings may be displayed by entering the appropriate commands:

```
ipepp;
ipgwp;
```

The configuration is displayed in the following format:

```
<ipepp;
ETH SPEED IPADDR          SUBNET          SCTP
1   AUTO  172.28.148.109  255.255.255.0   Y
2   AUTO  200.2.2.1       255.255.255.0   Y
3   AUTO  0.0.0.0         255.255.255.0   Y
4   AUTO  0.0.0.0         255.255.255.0   N
EXECUTED

<ipgwp;
IPGW    GATEWAY         MASK            IPNW
DEFAULT 172.28.148.1
EXECUTED
```

The new IP address parameters is initialized *with immediate effect*. If the IP address used to login to the unit for the telnet session is changed, you are automatically logged out of the session. You can however login again without delay using the new IP address.

> ***Note:*** Network infrastructure may introduce a delay while MAC addresses and newly configured IP addresses are reconciled.

The Ethernet connection should be verified by attempting to ping the SWS from a computer connected to the same Ethernet network, using the following command:

```
ping 123.124.125.126
```

If the SWS has been configured correctly, it responds to the ping and the host machine displays a message confirming communication with the SWS (the exact format and response of this message is operating system dependant).

If ping fails, check that the IP address was entered correctly and that there is no fault with the cabling to the SWS.

Once ping shows that the Ethernet connection is valid, it should be possible to access the management interface previously used on the VT100 compatible terminal via telnet. This is achieved by establishing a telnet session to port 8100 or 8101.

***Note:*** It is **not** possible to telnet to the standard telnet port 23.

For example, on a typical host console, the following command starts a telnet session to an SWS with an IP address of 123.124.125.126:

```
telnet 123.124.125.126 8100
```

The telnet terminal displays the MML interface prompt:

```
SS7G30(SWS) logged on at 2004-09-01 00:28:13
<
```

An optional password may be set to control remote access to the MML interface. This is done using the CNSYS command described in Chapter 6, “Management Interface”:

```
CNUAS:ACCOUNT=admin,PASSWORD=D1@logiC;,CONFIRM=D1@logiC;
```

If set, a user opening a telnet session to the MML interface is prompted to enter a password, for example:

```
(SWS) logged on at 2004-09-10 12:48:13
password:
```

***Note:*** The Signaling Server uses a static routing method for associating IP networks with Ethernet interfaces. In a network with multiple theoretical routing paths between an IP address on the SWS and IP address on the network, the SWS may transmit packets **to** an IP address through a different interface to that which receives packets **from** that same IP address. It is therefore quite possible for the SWS to be unable to route packets back to an IP address if a connection associated with the destination IP address is lost. See Section 3.6.1on page 29 for more information.

### 4.2.3 Software Download

Current information and Dialogic® DSI Signaling Server software downloads can be found at the following URL:

http://www.dialogic.com/support/helpweb/signaling

Your product left the factory with fully functional software installed. You are however recommended to check the above URL for any recent revisions, and install them before putting the product into service.

Since it is possible to source units from multiple supply channels, we recommend that each is checked to verify that all units in a delivery are at the same software revision. Proceed as follows:

1. Check the current software version running in the system (see the CNSWP MML command in Section 6.9, “Configuration Commands” on page 56, for more information).
2. Check the latest distribution file from the “SS7G3x” sections on the Dialogic® Signaling and SS7 Products download web site: http://www.dialogic.com/support/helpweb/signaling/.
3. If a download is required, then store the distribution file in an empty directory of your hard drive.
4. Follow steps detailed in Section 5.2, “System Software” on page 37 in order to update the system software.

### 4.2.4 Installing Software Licenses

This section describes how additional licenses are installed on a Signaling Server. Each Signaling Server is licensed to run specific components of the protocol stack. The STLCP command provides a printout that shows which components are licensed on a particular unit. Each unit is uniquely identified by a unit identity value, which is displayed as the UNITID parameter in the CNSYP command output.

The License File, purchased as described in Section 2.2, is a simple text file. The contents of the file are similar to the following:

```
FEATURE SWS_U_G30 dialogic 1.000 permanent uncounted \
HOSTID=000e0de513c4 SIGN="0004 9D4E 76CB EB0F 1B97 050A 01BE \
9F00 EB51 0B97 E61E C0A9 D62B AFEE D91F"
FEATURE TCAP_G30 dialogic 1.000 permanent uncounted \
HOSTID=000e0de513c4 SIGN="00F1 C40B AE29 A1B0 B4E5 1040 28B3 \
7F00 DFF2 146D E5D3 3F0D C281 72AD B0C4"
```

The license file should be installed on the Signaling Server product(s) as follows:

1. Rename the purchased license file to sgw.lic
2. Establish an FTP session (see Section 8.11.1, “Establishing an FTP Session” on page 170).
3. Set the FTP transfer mode to “ASCII”, since the license file is a text file.
4. Transfer the software license to the SWS by typing the command “put sgw.lic sgw.lic”.

   ***Note:*** The SWS uses a case-sensitive file system. Therefore, it is necessary to specify sgw.lic in lowercase.
5. Terminate the FTP session by entering “quit” or “bye”.
6. Establish an MML session and restart the unit by typing the “MNRSI” command.

   The machine then boots and completes the upgrade. Once the upgrade is complete, the machine is accessible via the MML interface.
7. Check the licenses using the CNSYP command and the STLCP command.

   If the licensing upgrade fails, the unit restores the previous licensing level. Further licenses can be added at a later date The license file containing these additional licenses should not contain licenses that have previously been installed.

### 4.2.5 Configuration Procedure

Once the system architecture and protocol configuration is known, it is necessary to set this configuration in the SWS.

The SWS is configured in two stages. Selection of protocol modules and assignment as either SWSA or SWSB is achieved using the CNSYS command described in Chapter 6, “Management Interface”. SS7 protocol and physical interface parameters are set by editing the *config.txt* file. See Chapter 8, “Configuration” for details. This can be transferred to the SWS via FTP or sFTP.

***Note:*** Note: Secure FTP users by default will land in the parent directory of siuftp and will need to change to the siuftp directory before commencing operation. Most Secure FTP clients provide an option to configure the default initial directory. If available, users may choose to use this instead of manually changing to the siuftp subdirectory.

You should connect to the FTP session as user name **siuftp** with an initial password set to **siuftp** or the password as set by the CNUAS command for the siuftp account.

# Chapter 5: System Management

## 5.1 Management Interfaces

The SWS system offers a number of management interfaces supporting the following functionality:

- Web-Interface
  Configuration and management of high-level protocol parameters for the mobile services being offered such as SMS, USSD and location based services. Also provides basic system information and statistics.
- MMI Console
  A console based interface over telnet or serial port to configure and manage many aspects of the system. Also provides easy access to diagnostic and statistics from the system.
- SNMP
  Optional interface supporting functionality for traps, alarms and other indications.

Refer to Chapter 6, “Management Interface” and Chapter 7, “Web-based Management Interface”

## 5.2 System Software

Unit software for the Dialogic® DSI SS7G31 and SS7G32 Signaling Servers may be updated by FTP transfer or from CD-R. Unit software for the Dialogic® DSI SS7G31 and SS7G32 Signaling Servers may be updated by FTP transfer or from USB.

Current information and file downloads for Signaling Server units can be found at the following URL:
http://www.dialogic.com/support/helpweb/signaling

Although updating the software is not a requirement and units are expected to function well with the software supplied with them, it is recommended that you use the latest version of the software available.

### 5.2.1 Updating the Software by FTP Transfer

The procedure to update the system software by FTP Transfer is as follows:

1. Establish an FTP session (see Section 8.11.1, “Establishing an FTP Session” on page 170).
2. Since this software is a binary file, set the FTP transfer mode to “BINARY”.
3. Transfer the SWS mode specific software binary by typing:

```
put ss7g30-sws.tgz sgw.tgz
```

***Note:*** The SWS uses a case-sensitive file-system. Hence, it is necessary to specify the name of the target file (the second filename in the example command shown above) in lowercase.

***Note:*** Different operating modes have different binary file names with ss7g30-sgw.tgz being used for SGW.

***Note:*** Software prior to Release 2.2.0 requires that the file being installed is of the name sgw.tgz. Release 2.2.0 or later will accept ss7g30-sws.tgz, ss7g30-siu.tgz, ss7g30-sgw.tgz or sgw.tgz.

4. The FTP session should then be terminated by entering the “quit” or “bye”.
5. Establish a MML session and restart the unit by typing “MNRSI:RESTART=SOFT”.

***Note:*** If you need to switch to SWS mode from some other mode after applying licenses, the command to use is: MNRSI:SYSTYPE=SWS RESTART=SOFT;

6. The machine then boots.
7. Once the upgrade is complete, the machine is accessible via MMI and the upgrade version can be checked using the CNSWP command.

### 5.2.2 Updating the software from USB (SS7G31 and SS7G32 Systems)

For SS7G31 and SS7G32 systems, the procedure for updating the system software from USB is as follows:

1. Copy the software binary distribution file to the USB memory device.
2. Insert the USB memory device into the USB port on the **front** of the unit.
3. Restart the unit using the **front** panel reset button, or by entering the **MNRSI**; MMI command.
4. The system will reboot until you are presented with the MMI command prompt.
5. Check the software version using the **CNSWP** command.
6. Remove the USB device from the USB port.

## 5.3 Diagnostics

The SWS supports built-in real-time logging to disk of activity on the MMI interface events and errors and the selective logging to disk of diagnostic traces.

Logging to disk of MMI activity events and errors by default allows a user to capture any management information at the point a failure occurs. Selective logging to disk of traces completes the capture of all the information that may be required to investigate particular issues.

Although activation of trace logging has a performance impact on a system, customers who do not require the full performance capabilities of the SWS may choose to activate selective tracing, such that the full capture of any significant information required for problem analysis.

To activate selective tracing, the user should first configure where they wish the trace messages to be logged using the CNSYx command TRACELOG parameter and then configure and activate the relevant trace mask using CNTMx commands. TRACELOG, by default, will be set to log trace messages to local FILE. The user can, however, modify the TRACELOG configuration to either transmit the messages to the management module on the management HOST or to DUAL to log locally as well as transmit to the management host.

Events and errors will be logged to files of the name “maint.log” in the syslog sub-directory of the siuftp account. These files will be limited to be a maximum of 5 MB with support being provided for up to 10 files. When the maint.log file reaches the 5 MB limit, or the system is restarted, it will be renamed maint.log.1 and a new maint.log file will be created. If there is an existing maint.log.1 file that will be renamed maint.log.2, other log files will consequently be renamed in a similar manner with the oldest file maint.log.9 being removed.

MMI inputs and outputs will be logged to files of the name "mmi.log" in the syslog sub-directory of the siuftp account. In the same manner as the maintenance logs, these files will be limited to be a maximum of 5MB with support being provided for up to 10 files.

When configured, trace messages will be logged to files of the name “trace.log” in the syslog sub-directory of the siuftp account. Just as with event and MMI logs, logs of these files will be limited to be a maximum of 5MB with support being provided for up to 10 files. Finally, trace messages for M3UA and MTP3 may also be logged in PCAP file format producing files of the name "trace.pcap'in the same manner as above. PCAP logging is selected using the TRACEFMT parameter in the CNSYx MMI command.

Upon restart, the SWS also backs up the existing system configuration and generates additional diagnostic files. These files, together with the maintenance and optionally trace log files may aid the support channel in the analysis of events and errors occurring on the SWS. The configuration files, maintenance and trace files as well as the additional text files, startup.logs and shutdown_logs can be recovered from the syslog directory using FTP protocol as described below.

```
ftp 123.123.123.123
user siuftp
password siuftp (or as set by the CNUAS command)
cd syslog
ascii
get config.txt *
mget startup.log*
mget shutdown.log
```

```
mget maint.log*
mget trace.log*
mget trace.pcap*
mget mmi.log*
bin
get config.CF1
bye
```

## 5.4 SNMP

### 5.4.1 Overview

The Signaling Server supports an extended SNMP offering comprehensive support for status and traps, Distributed Structure Management Information (DSMI) SNMP.

SNMP operation is disabled by default.

**Activating SNMP**

SNMP support can be activated by setting the CNSNS MMI command's SNMP parameter to **DSMI**.

The server should be restarted using the MNRSI command to activate the SNMP agent.

### 5.4.2 DSMI SNMP

DSMI SNMP functionality allows the configuration of V1 (RFC 1157), V2c (RFC 1901), or V3 (RFC 2571) SNMP traps notifying external SNMP managers of alarm conditions and configuration state changes for the objects supported on the MIB.

For all objects represented within the DSMI MIB — and these include platform hardware components as well as configuration aspects — the MIB will maintain current object state and alarm conditions affecting the object.

SNMP traps can be configured on a per-object basis such that the remote SNMP manager is notified whenever the object is created, destroyed or the object state changed. Traps can also be configured to notify the manager of events affecting the object. SNMP traps identify the event affecting the object — be it an alarm indication or configuration state change — and an event severity level.

For details of the DSMI SNMP MIB, supported alarms, SNMP traps and configuration refer to the *Dialogic® DSI Signaling Servers SNMP User Manual (U05EPP01)*.

## 5.5 Alarm Listing

A system operator can obtain a listing of the current alarm status (CLA, CATEGORY, ID and TITLE) of a Signaling Server using the ALLIP management terminal command described in Section 6.8.1, “ALLIP” on page 54. Table 1 details the possible alarm types accessed by the ALLIP command. Alarm status/events may also be accessed/reported by front panel LEDs, relay connections, API and SNMP, as described in Section 3.8, “Alarms” on page 29.

### Table 1. Possible Alarm Events

| Severity (LED) | TITLE | Description | CATEGORY | ID | CLA |
|---|---|---|---|---|---|
| Critical (CRT) | Board failed | A signaling board has failed.<br>For SS7HD board failure alarms, an additional diagnostic fault code may be displayed. This, when available, will follow the alarm title in ALLIP output and will be of the form “ ( fault code 0xnnnn )” - excluding the apostrophes and where nnnn is a 4 digit hexadecimal value. You should contact your support channel for further information. | SYS | Indicates board position. | 3 |
| | Configuration failed | The protocol configuration could not be completed due to errors in the configuration file | SYS | 0 | 3 |
| | Fan failure | CPU fan failure | SYS | 0 | 3 |
| | Fan warning | System fan failure | SYS | 0 | 3 |
| | Host link failed | Host (Ethernet) link has failed | SYS | HOSTID | 3 |
| | Memory failure | The system has detected that one or more of its memory modules has failed. | SYS | 0 | 3 |
| | PSU failure | Power supply has failed | SYS | PSU ID | 3 |
| | Restart error | An error was encountered processing the configuration file | SYS | Line number in configuration file where error was found | 3 |
| | Restart required | A system restart is required before system changes can take place | SYS | 0 | 3 |
| | SWS link failed | Inter SWS (Ethernet) connection has failed | SYS | 0 | 3 |
| | Switch error | This event indicates that boot switch on the SPCI4 board is set to an incorrect value. To correct set the switch to position 8. | SYS | Indicates board position | 3 |
| | System Overloaded | System Overload due to excessive network traffic | SYS | 0 | 3 |
| | Temperature | The internal temperature is outside a preset threshold indicating that either an internal fault or failure of the cooling arrangements. Inspection should take place immediately. | SYS | 0 | 3 |
| | Trial mode | The system is operating in trial mode and will reset after one hour | SYS | 0 | 3 |

| Severity (LED) | TITLE | Description | CATEGORY | ID | CLA |
|---|---|---|---|---|---|
| Major (MAJ) | AIS | Received data in SS7 timeslot all 1s on PCM trunk interface | PCM | PORTID | 4 |
| | CPU warning | The system has detected that one or more of the CPUs is likely to fail. | SYS | 0 | 4 |
| | Drive unavail | A disk drive in the RAID array is unavailable for use | SYS | DRIVE ID | 4 |
| | Parse errors | One or more syntax errors were found in the protocol configuration file | SYS | 0 | 4 |
| | PCM loss | No signal detected on PCM network trunk | PCM | PORTID | 4 |
| | RAI | Remote Alarm Indication received on PCM trunk interface | PCM | PORTID | 4 |
| | SS7 link failure | SS7 signaling link has failed | SIG | LINKID | 4 |
| | Sync loss | Unable to achieve frame synchronization on PCM trunk interface | PCM | PORTID | 4 |
| | Voltage warning | The system has detected that the voltage on one or more power rails is out of range. This is usually due to either a faulty power supply module or a faulty board causing excessive current consumption. | SYS | 0 | 4 |
| | SIGTRAN link failure | A SIGTRAN link has failed | SIG | SNLINK ID | 4 |
| Minor (MNR) | Default alarm | The system has detected a low priority low level alarm condition. You should contact your support contact for further information. | SYS | 0 | 5 |
| | Traffic congest | Traffic being processed by a throughput licensed protocol exceeds the license limits | SYS | PROTOCOL ID | 5 |
| | Traffic enforce | The system is acting to reduce traffic levels that exceed the throughput license limits | SYS | PROTOCOL ID | 5 |

## 5.6 Hard Disk Management

### 5.6.1 SS7G31 and SS7G32 Hard Disk Drive RAID Management

The SS7G31 and SS7G32 systems are equipped with 2 mirrored hard disk drives configured in RAID 1 array (Redundant Array of Independent Disks). These disks will remain synchronized, provides that an up-to-date copy of all data on the disk drives (such as the operating system software, Dialogic® DSI signaling software, system licenses and configuration files) will be maintained on both disks. In the event of failure of a single drive, the Signaling Server will continue to support the capabilities of the Signaling Server. When the failed disk drive is replaced with a unformatted disk drive, following the procedure below, the Signaling Server will mirror the operating software and data onto the new drive.

In the event of hard disk failure, the system will alarm, identifying the disk as unavailable. On SS7G31 systems, the disk drive must be deactivated using the MNINI command (see Section 6.12.1 on page 89) before the unit is shut down, and the hard drive removed and replaced. For the SS7G32, the disk drive must be deactivated but the unit does not require to be shut down.

Refer to hard disk drive removal instructions in the *Dialogic® DSI SS7G31 and SS7G32 Signaling Servers Hardware Manual*. Once the disk has been replace — and in the case of the SS7G31, the system restarted — the replacement drive should be activated using the MNINE command (see Section 6.12.2 on page 89), at which time the system will perform a synchronization function, copying all software to the newly installed disk drive. The “disk unavailable” alarm will persist until both disk drives are synchronized. The disk unavailable alarm will persist even if a failed disk drive is removed and not replaced.

Spare hard disk drives for the SS7G31 and SS7G32 system are available as on orderable part. Refer to the *Dialogic® DSI SS7G31 and SS7G32 Signaling Servers Product Data Sheet* (navigate from http://www.dialogic.com/products/signalingip_ss7components/signaling_servers_and_gateways.htm) for part number information.

***Important:*** Although the RAID management software has been designed to be robust, it is important to follow the removal and replacement procedures described above, in order for RAID array hard disk drive integrity.

***Warning:*** USB storage devices should not be connected to the Signaling Server during hard disk drive removal and replacement. Verify that all attached USB storage devices are removed before performing HDD removal, replacement and re-activation.

Disk drive replacement should be performed during a scheduled maintenance period and, for the SS7G32, which supports hot swap, during a period of light traffic. Re-synchronization of disk drives subsequent to replacement can take between 5-10 minutes, depending on the conditions and the load under which the Signaling Server is operating. The Signaling Server should not be restarted during this period and MMI activity should be limited to checking the status of the re-synchronization. The status of the disk drives can be identified using the STDDP command (see Section 6.15.5 on page 105). A status of UP indicates that a drive is fully operational, a status of DOWN indicates either that the disk is faulty or otherwise unable to synchronize. A status INACTIVE indicates that is has been deactivated by the user, a status of RESTARTING indicates that it is attempting to synchronize but the operation is not yet complete.

If the server is restarted through power loss or user action while synchronization is in progress, the synchronizing disk will be in an indeterminate state and on restart may cause the server to fail to boot. In such an event the disk should be removed from the server and any formatting on the disk manually removed. The disk should be re-installed on the server and the system booted. To restart synchronization you should deactivate (MNINI) and the re-active (MNINE) the disk. On the SS7G32 the disk does not need to be re-formatted instead you should simply boot without the disk, insert it when the system is operational and re-activate synchronization using MNINI/MNINE.

***Warning:*** Attempts to reactivate disks that have failed due to hardware reasons potentially can lead to a restart of the server. The server operates a watchdog to protect the operation of the server. If the server becomes unstable due to a failed hardware or software component, the watchdog will force a system restart to attempt to resolve the problem.

If a disk drive remains in the “DOWN” state after attempting re-activation, either the replacement drive is faulty or it has previously been formatted (RAID will only function with unformatted drives). In the case of the SS7G32, RAID mirroring may also fail and the disk remain “DOWN” due to the action of the hot-swap. If this occurs, the Server should be restarted and synchronization re-activated using MNINI/MNINE.

## 5.7 Secure Shell (SSH)

For additional security, the Signaling Server supports the use of Secure Shell (SSH) tunneling for telnet and secure FTP operation.

***Note:*** The unit does not provide a Secure Shell session connection. Your SSH client may need additional configuration to allow SSH tunneling without a session connection.

Once activated, a future user is required to set up an SSH tunnel prior to telnet access. For a client on a Linux- or Solaris-like operating system, log in for telnet using the ssh application. The ssh application should be invoked using a shell script of the following form:

```
#!/bin/sh
ssh -l siuftp -C -f $1 -L 2323:$1:8101 sleep 5
telnet localhost 2323
```

For a client on a UNIX operating system, the command sequence to log in for FTP access using the sftp application is:

```
sftp -l siuftp@<SWS IP Address>
```

You are also prompted to enter the password for the siuftp login account.

The secure connection to a unit can also be established from other operating systems, using the appropriate SSH software.

### 5.7.1 Configuring Public-Key Authentication for SSH

Configuring for Public-Key Authentication allows the operator to use SSH to connect to the SWS without using a password. For security reasons this is recommended where the connection is made using a script.

This process requires an RSA or DSA key-pair generated for each Host. Refer to the documentation for the SSH package for more information.

- "Using Secure FTP to connect to the SWS.
- "If the ".ssh" directory does not exist in the siuftp account, create one.
- "Create a text file and add the Public Key for each Host on a new line.
- "Upload the file to ".ssh/authorized_keys".
- "Ensure the permissions on the ".ssh" directory and its parent directory "siuftp" are set to "750".
- "Ensure the permissions on ".ssh/authorized_keys" are set to "640".

It is recommended that the first connection using the Public-Key Authentication method be made manually.

When using SSH or Secure FTP to connect to the Signaling Server, specifying the Private-Key will allow you to log in as siuftp, without using the password.

### 5.7.2 SSH Tunneling for RSI

To protect RSI traffic between the SWS and SWS-Host, the SWS-Host may be configured to use an SSH tunnel to transport the RSI traffic to the SWS.

The configuration of the SSH Client on each SWS-Host depends on the SSH package used. The following instructions show a suggested configuration method for both Linux and Windows® operating systems. For both systems, it is recommended that the first connection is made manually, to allow the Client accept the SWS Host Key.

#### 5.7.2.1 Using Linux and OpenSSH

The following script initiates a single SSH tunnel. The SSH Client exits, rather than attempting to re-establish the tunnel, should the IP link be interrupted or the SWS restarted, so the loop provides that the SSH client is restarted. This configuration may also be used with Solaris and Sun SSH.

tunnel.sh contains:

```
#!/bin/sh
#tunnel.sh - configures a SSH tunnel to the SWS ($1).
while true
do
  ssh -l siuftp -i ~/.ssh/priv_key -N -C -L 9000:$1:9000 $1
done
```

The tunnel script is started, prior to starting the GCT environment, with the command:

```
./tunnel.sh <SWS IP Address>
```

#### 5.7.2.2 Using Windows® and PuTTY

The following script initiates a single SSH tunnel. The SSH Client does not attempt to re-establish the tunnel should the link be interrupted, so the loop provides that when the SSH client returns it is started again.

tunnel.bat contains:

```
REM tunnel.bat - configures a SSH tunnel to the SWS (%1)
:start
  plink.exe -ssh -l siuftp -i priv_key.ppk -batch -N -C -L 9000:%1:9000 %1
goto start
```

The tunnel batch file is started, prior to starting the GCT environment, with the command:

```
tunnel.bat <SWS IP Address>
```

### 5.7.3 General Notes

Your SSH Client may keep a list of "known hosts". The first time SSH connects to an SWS the SSH Client will prompt to accept the Host Key. The Client may also warn if the Host Key changes. This would occur if the SWS is move to a different IP address or if the Hard Disk is replaced.

#### 5.7.3.1 SWS MMI Interface

The SWS will report that the Foreign IP address is the same as the SWS IP Address in the STHLP command.

```
Host link status
HOSTID       RSI STATE     FOREIGN IPADDR          TCP STATE
0            *ACTIVE       192.168.0.1             ESTABLISHED
EXECUTED
```

#### 5.7.3.2 Supported Ciphers

The Signaling Server uses OpenSSH_3.5p1 to provide SSH functionality and supports the following ciphers: 128 bit AES, Blowfish, 3DES, CAST128, Arcfour, 192 bit AES, or 256 bit AES. Refer to the SSH Client documentation for details for how the cipher may be specified.

### 5.8 System Backup and Restoration

You can back up the system configuration, software licenses, and operating software to an archive which can be restored to the system at a later date.

At startup the system will take a copy of the following system files storing them in the syslog subdirectory of the siuftp account:

| File | Description |
|---|---|
| ss7g30.tgz | A binary file containing pre Release 2.2.0 operating software if present. |
| ss7g30-sws.tgz | A binary file contain SWS mode operating software, if present |
| ss7g30-siu.tgz | A binary file contain SIU mode operating software, if present. |
| ss7g30-sgw.tgz | A binary file contain SGW mode operating software, if present. |
| sgw.lic | A text file containing the current software licenses active on the system, if present. |
| modcap | A binary file containing a software license allowing Signaling Server operating software to function on this particular system. |
| config.CF1 | A binary configuration file containing dynamically configurable data that is common to all modes of operation. Parameters set by the CNSYS command would for example be stored in this file. |
| config.txt | The text configuration file for an SWS or SIU, if present. |
| SDC.CF3 | The binary configuration file for a SGW, if present. |

The files can be recovered from the syslog directory using FTP as detailed below:

```
ftp 192.168.0.1
user siuftp
password ********
cd syslog
ascii
get config.txt
get sgw.lic
bin
get sgw.lic
get modcap
get config.CF1
get SDC.CF3
get SDC.CF4
cd dist
get ss7g30.tgz
get ss7g30-siu.tgz
get ss7g30-sgw.tgz

bye
```

You may then archive these files by transferring them to an ISO9660 format CD or USB.

To validate that a software license (modcap) has been created without error, you may put the portable media into the Signaling Server and type the following command:

```
CNUPI:DTYPE=SYSKEY;
```

If the command returns 'EXECUTED' then the portable media contains a valid software license.

A Signaling Server may be restored to the configuration and licensing stored on the portable media by inserting the portable media (CD or USB) into the Signaling Server and re-booting. On re-boot, the system will install the files stored on CD or USB onto the system. Configuration files present on the portable media will overwrite any in the SIUFTP directory.

***Note:*** Once the system has been restored, you must ensure that the CD or USB is removed from the Signaling Server, otherwise on subsequent re-boot the system will again install the files stored on portable media.

If you change dynamically configurable data on the system using MMI (i.e., MMI commands described in the user manual with the attribute “CONFIG”), you may wish to create a new backup of the config.CF1 file containing the new configuration data to the syslog directory in the siuftp account. To do so without restarting the system, type the following command:

```
CNBUI:DTYPE=SYSCFG;
```

Following this command a new portable media archive should be created, following the procedures identified above.

***Note:*** You also have the ability to re-install any of the previously backed up system files (identified above) or to install a new text configuration file using FTP rather than from portable media. In this case, they should ftp the files onto the unit using the procedures defined in this manual.

## 5.9 SIGTRAN Throughput Licensing

The SIGTRAN license installed on the unit determines the number of SIGTRAN links that can be configured on the system. For license descriptions, see Section 2.2, “Software Licenses” on page 17.

Throughput is restricted through a congestion mechanism which allows a system to briefly exceed the licensed throughput - provided that the average throughput does not exceed the licensed limit. If a system exceeds the limit for a sustained period of time then the licensed limit will be enforced and traffic throttling will reduce throughput until sufficient credit is gained to return to normal operation.

Two alarms provide indications of throughput congestion and throughput enforcement. Traffic congest indicates that enforcement will be reached unless traffic is reduced, Traffic Enforce indicates that the system is actively throttling the traffic to the licensed rate. In addition, the API command API_MSG_SIU_STATUS, will provide the following indications of congestion and enforcement to the management module.

| Value | Event | ID |
|---|---|---|
| 0x2b | Traffic congestion | 0 |
| 0x2c | Traffic enforcement | 0 |
| 0x2d | Clearing traffic congestion and enforcement if active. | 0 |

The MMI command, STLCP, will report the status of the licensable capabilities of the system such as protocols or different modes of operation. The command will report whether a license is present, whether it is inactive or active, whether it is dependant on another license or requires a restart before it can become active. The STLCP command also reports the permitted throughput and remaining throughput credit. The MMI command, MSLCP provides measurements showing peak and total throughput within a particular time period.

# Chapter 6: Management Interface

The management interface is accessed by a remote telnet session to port **8100** or **8101**.

For maintenance purpose the unit may also be accessed from a VT100-compatible terminal connected to the serial port of the equipment (COM 2 on the back of the unit). The serial port operates at 9600 baud, 1 stop bit, 8 data bits, no parity.

When the session is established, a welcome message containing the software product name, mode of operation (SWS), the system identification string (SYSID), the date and time is displayed:

```
SS7G31 (SWS) <SYSID> logged on at <calendar date> <time of day>
```

## 6.1 Log On/Off Procedure

To initiate a dialog the operator must *log on* to one of the MML interfaces.

The two telnet connections provided are accessed using a standard telnet utility. Ports 8100 or 8101 should be used for the connection (rather than port 23, the default port).

To log onto a serial port, the carriage return key should be entered. The session is ended by an operator command to the SWS or at the expiry of an auto log off timer.

If a password is specified for the system, then when logging on the password is required before being allowed to continue. If an incorrect password is entered, the system prompts again for a password. If an incorrect password is entered 3 times, then the port is disconnected. For safety reasons, the password is never required for the serial port (COM 2).

When the connection has been established, the command prompt is output, which is the *less than* symbol (<). The log on session is ended either by operator command or at the end of an auto log off timeout.

The system maintains two timers during the log on session:

- An *auto log off warning* timer
- An *auto log off* timer

Both are restarted each time a new command is input. When the auto log off warning timeout expires, an auto log off warning message is output to the terminal and any partially entered command discarded. The system then outputs a command prompt to the terminal. If no command is input before the auto log off timeout expires, the log on session is ended.

When log off is initiated, a message containing the software product name, mode of operation (SWS), the system identification string (SYSID), the date and time is displayed:

```
SS7G32 (SWS) <SYSID> logged off at <calendar date> <time of day>
```

The SWS then initiates the appropriate procedure to end the connection to the operator's terminal.

## 6.2 Command Entry

Commands may be entered whenever the command prompt "<" has been output. Commands are terminated by a semicolon (;) followed by a carriage return (CR).

If a command takes parameters, a colon (:) is used to separate the command from the parameters. A comma (,) is used to separate multiple parameters. Table 3, "Parameter Definitions" on page 48 gives information on command parameters and describes their format and permissible value ranges.

Commands that affect operation are considered *dangerous* commands. If a dangerous command is entered, the SWS outputs the following on a new line:

```
Are you sure? [Y/N]
```

The operator must enter **Y** to continue the execution of the command. Any other valid input causes the command to be aborted.

A summary of the available commands is given in Section 6.17, “Command Summary” on page 121. Command details are given in Section 6.8 through Section 6.15.

## 6.3 Command Responses

The SWS does not produce output except in response to an operator command. When a syntactically correct command has been issued, acceptance is indicated by the Executed Response output as follows:

```
EXECUTED
```

An invalid command is not acted upon. The SWS indicates command rejection by issuing one of the responses listed in the Table 2:

**Table 2. Command Responses**

| Response | Reason for Rejection |
|---|---|
| EXTRA PARAMETERS | Too many parameters have been entered. |
| GENERAL ERROR | Command unable to execute due to external error. |
| ILLEGAL COMMAND | The command is invalid for the mode of operation. |
| INVALID INDICATOR | The command code contains an invalid indicator. |
| INVALID PARAMETER NAME | A parameter name has been entered which is not valid for this command. |
| MISSING PARAMETER | A required parameter has not been input. |
| NO SYSTEM RESOURCES | The requested command cannot be executed because the unit is busy processing another command. This response may also be given during restart when the system is initializing. |
| RANGE ERROR | A parameter value is out-of-range. |
| UNACCEPTABLE COMMAND | The command is syntactically correct, but references an unknown resource (board, link etc.) |
| UNKNOWN COMMAND | The command is not recognized. |

## 6.4 Automatic MMI Logging

To allow for audit of user MMI sessions, all user dialogues are logged to a rolling log file to permit subsequent review of the command history. The text format log files include all MMI commands, responses and events.

Log files are created in the 'syslog' sub-directory of the siuftp account. The most recent file is called mmi.log and older files are called mmi.log.1, mmi.log.2 and so on up until mmi.log.9. The capacity of each file is limited to prevent disk overflow.

Each entry in the file includes the date and time of the event. For security, the text value of the PASSWORD and CONFIRM parameters are replaced by the string "******".

## 6.5 Parameters

All numeric parameters are entered and output in decimal notation. The following table lists parameters and possible values:

**Table 3. Parameter Definitions**

| Name | Description |
|---|---|
| ACTIVE | Determines whether something is active “Y” or inactive “N”. An example of its use is the activate or deactivation of trace masks (see the CNTMS command). |
| AUTH | V3 SNMP Authentication encryption protocol - used to provide that V3 SNMP requests have not been modified during transit. Set to SHA or MD5. |
| AUTHPASS | SNMP V3 User account Authentication password. Must be set if the AUTH parameter is set. minimum of 8 chars max 12 characters |
| BIND | Logical identifier for a binding between a Local Application Server and either a Remote Application Server or Remote Signaling Gateway. The valid range is 0-199. |
| BPOS | Board position in the range 1 to 3<br>**NOTE:** An Signaling Server with two boards has the boards installed in positions 1 and 3. |

## Table 3. Parameter Definitions (Continued)

| Name | Description |
|---|---|
| CATEGORY | Alarm category:<br>• SYS - a system alarm<br>• PCM - a pcm alarm<br>• SIG - a signaling alarm<br>See Section 5.5, "Alarm Listing" on page 40 for more information. |
| CLA | Alarm class:<br>• 5 - a minor MNR alarm (triggers the MNR LED alarm)<br>• 4 - a major MJR alarm (triggers the MJR LED alarm)<br>• 3 - a critical CRT alarm (triggers the CRT LED alarm)<br>See Section 5.5, "Alarm Listing" on page 40 for more information. |
| CLASS | Requests help output for either PARAMETERS or ERRORS. PARAMETERS are those specified in this table; ERRORS are those specified in Section 6.3, "Command Responses" on page 48 |
| CMD | MML command name. See Section 6.17, "Command Summary" on page 121 for a complete list of MML command names. |
| CONFIRM | Confirmation of the PASSWORD typed for remote access to MML interface sessions.<br><br>To provide that only strong passwords are used the following rules will be enforced:<br>• The password must not be the same as any of the previous 8 passwords used.<br>• It must be between 8 and 15 characters.<br>It must have at least 1 upper case character, 1 lower case character, 1 digit and one special character. Special characters support are:<br><br>~ $ % ^ @ # |
| CONTACT | Label identifying person/group responsible for the Signaling Server. Maximum 24 characters e.g email@example.com |
| CSSR | A concerned SCCP sub-system resource, that is, a sub-system resource that wants to receive state change information about another SCCP sub-system or signaling point. Possible values are:<br>• LSS - Local Sub-System<br>• RSS - Remote Sub-System<br>• RSP - Remote Signaling Point |
| DATE | Calendar date in the format xxxx-yy-zz, where:<br>• xxxx is a four digit year value (in the range 1990 to 2038)<br>• yy is a two digit month value (in the range 1 to 12)<br>• zz is a two digit day value (in the range 1 to 31) |
| DLGID | A logical identifier for a TCAP dialog, The valid range is 0 to 65535. |
| DMHOST | The default management host. In the range of 0 (default) to 63. |
| DRIVE | A Drive bay identifier for a disk drive; value in the range 0 to 1. |
| DTYPE | A type parameter identifying the item to backed up/updated. Possible values are:<br>• SYSKEY - The system license (modcap)<br>• SYSCFG - The binary system configuration (config.CF1)<br>• CONFIG - The text configuration (config.txt) |
| DOWN | SNMP object transition state: Traps will be generated if set to All, Create, Change or Destroy. Traps will not be generated if set to NONE. Default = Change |
| END | identifies whether the SWS end of the SIGTRAN link acts as a client or server. Possible values are C or S. |
| ENGINE | V3 SNMP Identifies the Engine part of the remote SNMP entity (manager). Max 24 hexadecimal characters. |
| ETH | Ethernet port number in the range 1-6 |
| FTPPWD | FTP Password enabled parameter. Set to "Y" to enable FTP password protection, or "N" to disable password protection. |
| FTPSER | FTP server activate. Set to "Y" to active the ftp server, or "N" to disable the ftp server. |
| GATEWAY | Address of an IP gateway, in the form aaa.bbb.ccc.ddd.<br>Set to 0.0.0.0 to indicate that no gateway is present. |
| HOSTID | Logical ID of an SWS host, in the range 0 to 63. |
| HPORT | Host SCTP port in the range 1 to 65535. |
| ID | Command-specific ID parameter. |
| IMASK | Input Mask; a trace mask for signaling messages entering a protocol module. |

## Table 3. Parameter Definitions (Continued)

| Name | Description |
|---|---|
| IMPAIR | SNMP object transition state: Traps will be generated if set to All, Create, Change or Destroy. Traps will not be generated if set to NONE. Default = Change |
| INACTIVE | SNMP object transition state: Traps will be generated if set to All, Create, Change or Destroy. Traps will not be generated if set to NONE. Default = Change |
| INHIBIT | Set to“Y” to inhibit an SS7 link or set to “N” to uninhibit the link. |
| IP1 | The primary IP address on which the SWS will attempt to communicate with the peer unit. |
| IP2 | The secondary IP address on which the SWS will attempt to communicate with the peer unit. |
| IPADDR | The SWS’s own network IP address or that of one of it’s hosts, in the format aaa.bbb.ccc.ddd |
| IPGW | A logical reference for an Internet Protocol Gateway; value in the range 1 to 31. The gateway can also be specified as “default”. |
| IPNW | An IP network identifier, in the format aaa.bbb.ccc.ddd |
| LAS | Local Application Server. Logical reference for a Local Application Server. The valid range is 0-199. |
| LABEL | A text label used to identify the related item - 0 to 12 alpha-numeric characters. |
| LEDID | Front panel LED ID. Reserved for future use. |
| LINK | SS7 link identifier in the range 0 to 127. |
| LOCATION | Label identifying the location of the unit. Max 24 characters. |
| M2PA_ID | SIGTRAN SCTP association identifier in the range 0-32. For use with M2PA only. |
| MAP | MAP present parameter. Set to “Y” to enable the operation of MAP (when the software is licensed) or “N” to disable the operation of MAP. |
| MASK | An IP network mask, in the format aaa.bbb.ccc.ddd |
| MMASK | Management Mask; a trace mask for management messages generated by a protocol module. |
| MNGR | Logical identifier for an SNMP manager in the range 1-32. |
| MODE | Command-specific mode parameter. Value can be one of the following:<br>• SIUA or SIUB<br>• CGRP, MTPR, MTPLS, MTPL, MONL, LIU, SSR, CSSR, M3UAR or M3UARLIST<br>See the MMI commands for more information. |
| MODULE | Protocol module name. Permissible values are: MTP, TCAP, MAP, M3UA and SCCP. |
| NA | Network Appearance used when communicating with a remote server. Valid range is 0:16777215 |
| NASP | The number of ASP (SIGTRAN Links) required in load sharing mode. |
| NC | Or NC_ID. SS7 Network Context. The Network Context, together with a Signaling Point Code (SPC), uniquely identifies an SS7 node by indicating the specific SS7 network it belongs to. The Network Context may be a unique identifier for a physical SS7 network or may be used to subdivide a physical SS7 network into logical parts. Possible values are NC0, NC1, NC2 or NC3. |
| NTP | NTP activation parameter. Set to 'Y' to enable use of Network Time Protocol or 'N' disable use of Network Time Protocol. |
| NTPSER | Identifier for the NTP server. In the range 0 to 15. |
| OBJECT | Identifier of a table within a Signaling Server Group Object. Refer to the *Dialogic® DSI Signaling Servers SNMP User Manual* (U05EPP01) for MIB details. |
| OBJGRP | Identifier of the Signaling Server Group Object in the DSMI MIB:<br>1 - Management Group, 2 - System Group, 3- Platform Group, 4 - IP Group, 5- Board Group, 6 - SS7 Group, 7 SIGTRAN Group, 8 - Access Group. Refer to the *Dialogic® DSI Signaling Servers SNMP User Manual* (U05EPP01) for MIB details. |
| OFFSET | The OFFSET value must be specified in hours and optionally 0 or 30 minutes, in the range -14 to +12. The OFFSET is specified in POSIX-style, which has positive signs west of Greenwich. |
| OMASK | Output Mask; a trace mask for signaling messages leaving a protocol module. |
| PAGE | The page of data to be printed. |

## Table 3. Parameter Definitions (Continued)

| Name | Description |
|---|---|
| PASSWORD | Password for remote access to MML interface sessions.<br><br>To provide that only strong passwords are used the following rules will be enforced:<br>• The password must not be the same as any of the previous 8 passwords used.<br>• It must be between 8 and 15 characters.<br>It must have at least 1 upper case character, 1 lower case character, 1 digit and one special character. Special characters support are:<br><br>~ $ % ^ @ # |
| PORT | SNMP destination port for SNMP traps. Default 162. |
| PPORT | Peer SCTP port in the range 1 to 65535. |
| PRIV | SNMP V3 Privacy encryption protocol. Set to DES or AES |
| PRIVPASS | SNMP V3 User account Privacy password. Must be set if the PRIV parameter is used. minimum of 8, maximum of 12 characters |
| QUIESCE | SNMP object transition state: Traps will be generated if set to All, Create, Change or Destroy. Traps will not be generated if set to NONE. Default = Change |
| RANGE | A range parameter with valid values between 0 to 65535. An example of its use is specifying a range of TCAP dialogs to be printed by the STTDP command. |
| RAS | Remote Application Server identifier. |
| RASLIST | Logical identifier for a RAS to SNLINK relationship. The valid range is 0-6399. |
| RC | The logical routing context of the local application server. An RC might not be associated with any other LAS. The valid range is 0: 2147483647. |
| RCOM | Read only Community String. A maximum 12 alphanumerical characters. If configured the SNMP agent will silently discard any PDU for which the community string is not identical. If not configured the SNMP agent will respond to all received PDUs. Default value = “private”. |
| RESET | Performs a reset operation when set to “Y” An example of its use is the resetting of measurements to 0 using the MSPCP command. |
| RESTART | Specifies the type of restart operation, which can be one of the following:<br>• NORMAL - The system undergoes a full system restart, resetting the hardware, operating system and SWS software. This is the default behavior. NORMAL resets should be used for software upgrade or for maintenance events.<br>• SOFT - The system restarts the application software. Prior to a soft restart, the signaling boards are reset. SOFT resets may be used for a more rapid system restart after updating the system configuration or licenses. However, if a new software distribution is to be installed, the system performs a NORMAL restart.<br>• HALT - The system shuts down without a subsequent restart.<br>**Caution**: **Once the system has been halted, the only way to restart the unit is by physically pressing the Power switch on the front panel of the chassis.** |
| | SNMP object transition state: Traps will be generated if set to All, Create, Change or Destroy. Traps will not be generated if set to NONE. Default = Change |
| ROUTE | Logical reference for a SIGTRAN Route. The valid range is 0-199. |
| RSERVER | Remote Server. Identifies a remote server to act as a Remote Signaling Gateway. The remote server might not have the same id value as an existing Remote Application Server. No more than 32 SNLINKs can identify the same Remote server. All Sigtran links between the SWS and a Remote Signaling Gateway must be of the same protocol type. The valid range is 0-199. |
| RSG | Identifier of the remote signaling gateway. |
| RSGLIST | Logical identifier for a SIGTRAN Route to Signaling Gateway relationship. The valid range is 0-6399. |
| SCCPCL | SCCP “connectionless” operation present parameter. Set to “Y” to enable the operation of connectionless SCCP (when the software is licensed) or “N” to disable the operation of connectionless SCCP. |
| SCCPCO | SCCP “connection-orientated” operation present parameter. Set to “Y” to enable the operation of connection-oriented SCCP (when the software is licensed) or “N” to disable the operation of connection-oriented SCCP. |
| SCTP | SCTP availability. Set to “Y” to enable SCTP operation on a particular IP port. Set to “N” to disable SCTP operation on a particular IP port. |
| SECURE | SECURE operation. You can specify whether you wish to restrict access to the SWS so that it operates only over secure shell (SSH) by use of the SECURE parameter. Setting this parameter to “Y” increases the security level in a command-specific manner. By default there is no restriction, allowing the normal use of telnet and FTP. |
| SNLINK | SIGTRAN link identifier in the range 0 to 255. |
| SNMP | SNMP active parameter. Set to “Y” to enable operation of SNMP or “N” to disable operation of SNMP. |
| | SNMP version running of the system, Set to DK4032, DSMI or NONE. |

## Table 3. Parameter Definitions (Continued)

| Name | Description |
|---|---|
| SNRT | The SIGTRAN route identifier. |
| SPEED | The speed of an Ethernet port, which can be set to AUTO, 10, 100, 1000, 10H, 100H, where H indicates it is half-duplex, otherwise it is full-duplex. |
| SS7MD | Identifies the point code type used within the network context. Possible values are<br>ITU14 - ITU 14 bit operation<br>ITU16 - ITU 16 bit operation<br>ITU24 - ITU 24 bit operation<br>ANSI - ANSI 24 bit operation |
| SSR | An SCCP sub-system resource. Possible values are:<br>• LSS - Local Sub-System<br>• RSS - Remote Sub-System<br>• RSP - Remote Signaling Point |
| SSN | Subsystem number in the range 1 to 255. |
| SUBNET | IP sub-net mask for IPADDR (ENET 1); set by default to 255.255.255.0. |
| SYSID | An optional text string of length 0 to 12 characters long that can be used to help identify the unit. |
| SYSREF | An optional system reference number, in the range 0 to 999. The default value is 0. |
| SYSTYPE | The mode of operation of the system. Possible operating modes are:<br>• SWS – Signaling Web Services<br>• SGW – SIGTRAN Signaling Gateway<br>• SIU – Signaling Interface Unit |
| TCAP | TCAP present parameter. Set to “Y” to enable the operation of TCAP (when the software is licensed) or “N” to disable the operation of TCAP. |
| TCOM | SNMP Trap Community String A maximum 12 alphanumerical characters |
| TFORMAT | Format of SNMP trap to be dispatched to the SNMP manager: 1 - SNMP V1, 2 - SNMP V2, 3 - SNMP V2 INFORM. |
| TIME | Time of day in the format xx:yy:zz, where:<br>• xx is a two digit hour value (in the range 00 to 23)<br>• yy is a two digit minute value (in the range 00 to 59)<br>• zz is a two digit second value (in the range 00 to 59) |
| TITLE | Title describing alarm event. See Section 5.5, “Alarm Listing” on page 40 for more information. |
| TRACEFMT | TRACEFMT is used to specify the format of the log files written to local log on the SWS. Logs. It is defined as the following values:<br>• TEXT (default).<br>• PCAP<br>• DUAL (where PCAP and TEXT log files will be created). |
| TRACELOG | TRACELOG controls whether tracing to log or host is allowed. It is defined as follows:<br>FILE (default) - Trace messages will be locally logged but not transmitted to the management host.<br>HOST - Trace messages will be transmitted to the management host but not locally logged.<br>DUAL - Trace messages will be transmitted to the management host and also locally logged.<br>**NOTE:** Tracing is activated on a per protocol basis using the CNTMS command. |
| TRMD | The traffic mode for the local application Server. Acceptable values are LS (Loadshare), OR (Override) or BC (Broadcast). N.B. Only Loadshare should be used when the SWS is acting as part of a SWS Pair. |
| TYPE | Type of SIGTRAN link: M2PA or M3UA |
| UNITID | Unique identifier for this unit, used for licensing. A string of 12 hexadecimal characters. |
| UP | SNMP object transition state: Traps will be generated if set to All, Create, Change or Destroy. Traps will not be generated if set to NONE. Default = Change |
| USER | SNMP V3 Logical identifier for an SNMP user account in the range 1-32. |
| WARNING | SNMP object transition state: Traps will be generated if set to All, Create, Change or Destroy. Traps will not be generated if set to NONE. Default = Change |
| WCOM | Read/Write Community String. The Signaling Server SNMP agent will silently discard received PDUs that have a community string not identical to this value. A maximum 12 alphanumerical characters. Default value = “private”. |

## 6.6 Command Conventions

The following conventions are used in the command definitions:

- Items in square brackets [ ] are optional.
- Items separated by a vertical bar | are alternatives, only one of which may be used.
- Curly brackets { } are used to designate a group of optional items of which at least one must be selected.
- A parameter is specified using the parameter name followed by the “equal to” symbol (=) followed by the value of the parameter, with no intervening spaces.

The following symbols are used to indicate command attributes:

- **‘Prompt’** A *dangerous* command that must be confirmed by the operator.
- CONFIG - The command affects configuration data.

## 6.7 Commands

The following types of commands are listed in this chapter:


- Alarm Commands
- Configuration Commands
- IP Commands
- MML Commands
- Maintenance Commands
- Measurement Commands
- Reset Command
- Status Commands


A command summary is provided in Section 6.17, “Command Summary” on page 121.

## 6.8 Alarm Commands

The alarm commands include:

- ALLIP - Alarm List Print
- ALTEE - Alarm Tet End
- ALTEI - Alarm Test Initiate

### 6.8.1 ALLIP – Alarm List Print

#### Synopsis

This command gives a printout of ACTIVE fault codes stored in the system's alarm log.

See Section 5.5, "Alarm Listing" on page 40 for the definitions of the alarm TITLE.

#### Syntax

```
ALLIP;
```

#### Prerequisites

None.

#### Attributes

None.

#### Example

```
ALLIP;
```

#### Output Format

```
Alarm List (active alarms)
CLA CATEGORY  ID  TITLE
5   PCM       0   PCM Loss
5   PCM       1   PCM Loss
5   SIG       0   SS7 link failure
5   SIG       1   SS7 link failure
4   SYS       0   Host link failed
```

***Note:*** Table 1, "Possible Alarm Events" on page 40 details the possible alarm reports. The interpretation of the ID field in the listing is dependent on the value in the TITLE field.

### 6.8.2 ALTEE – Alarm Tet End

#### Synopsis

Clears a test alarm.

#### Syntax

ALTEE:{[CLA=5]|[CLA=4]|[CLA=3]};

#### Prerequisites

The alarm test must already have been initiated.

#### Attributes

None

#### Examples

ALTEE:CLA=3;

### 6.8.3 ALTEI – Alarm Test Initiate

#### Synopsis

The command generates an active test alarm of the specified class, which is entered in the alarm log. Alarm tests can be useful for validating the operation of hardware such as LEDS and alarm relays.

#### Syntax

ALTEI:{[CLA=5]|[CLA=4]|[CLA=3]};

#### Attributes

None

#### Examples

ALTEI:CLA=3;

## 6.9 Configuration Commands

The configuration commands include:

- CNBOP - Configuration Board Print
- CNBUI - Configuration Backup Initiate
- CNBUS - Configuration Backup Set
- CNCRP - Configuration MTP Route Print
- CNCSP - Configuration Concerned Subsystem Print
- CNGAP - Configuration GTT Address Print
- CNGLP - Configuration SIGTRAN Gateway List
- CNGPP - Configuration GTT Pattern Print
- CNGTP - Configuration Global Title Translation Print
- CNLSP - Configuration MTP Linkset Print
- CNMLP - Configuration Monitor Link Print
- CNOBP - Display TRAP Configuration
- CNOBS - Set TRAP Configuration
- CNPCP - Configuration PCM Print
- CNRDI - Configuration Restore Defaults Initiate
- CNSLP - Configuration SS7 Link Print
- CNSMC - Change SNMP Manager Configuration
- CNSME - End SNMP Manager Configuration
- CNSMI - Set SNMP Manager Configuration
- CNSMP - Display SNMP Manager Configuration
- CNSNP - Configuration SNMP Print
- CNSNS - Configuration SNMP Set
- CNSRP - Configuration SIGTRAN Route Print
- CNSSP - Configuration Subsystem Resource Print
- CNSTP - Configuration SIGTRAN Links Print
- CNSWP - Configuration Software Print
- CNSYP - Configuration System Print
- CNSYS - Configuration System Set
- CNTDP - Configuration Time and Date Print
- CNTDS - Configuration Time and Date Set
- CNTMP - Configuration Trace Mask Print
- CNTMS - Configuration Trace Mask Set
- CNTPE - Configuration Network Time Protocol Server End
- CNTPI - Configuration Network Time Protocol Server Initiate
- CNTPP - Configuration Network Time Protocol Print
- CNUAP - Configuration User Account Print
- CNUAS - Configuration User Account Set
- CNUPI - Configuration Update Initiate
- CNURC - Configuration Update Resource Change
- CNURE - Configuration Update Resource End
- CNURI - Configuration Update Resource Initiate
- CNUSC - Change SNMP v3 User Configuration

- CNUSE - End SNMP v3
- CNUSI - Set SNMP v3
- CNUSP - Display SNMP v3

### 6.9.1 CNBOP – Configuration Board Print

#### Synopsis

This command displays the configuration of all Dialogic® DSI SS7 Boards.

#### Syntax

CNBOP;

#### Prerequisites

None

#### Example

CNBOP;

#### Output format:

```
Board Configuration
BPOS    BTYPE       FLAGS
1       SPCI4       Ox0041
3       SPCI4       Ox0041

Where:
    BPOS - Board position
    BPOS - Board type
    FLAGS - Board Flags
```

### 6.9.2 CNBUI – Configuration Backup Initiate

#### Synopsis

This command is used to create a local backup (internally stored) of the existing protocol configuration file (config.txt) before an edit session.

#### Syntax

```
CNBUI;
```

#### Prerequisites

None.

#### Attributes

None.

#### Example

```
CNBUI;
```

### 6.9.3 CNBUS – Configuration Backup Set

#### Synopsis

This command is used to restore the protocol configuration file (config.txt) from the previously backed-up state.

### Syntax

```
CNBUS;
```

### Prerequisites

None.

### Attributes

CONFIG - The command affects configuration data.

### Example

```
CNBUS;
```

## 6.9.4 CNCRP – Configuration MTP Route Print

### Synopsis

This command displays the current MTP route configuration. See Section 8.6.7, “MTP_ROUTE” on page 146 for descriptions of the parameters in the output format.

### Syntax

```
CNCRP:[ID=];
```

### Prerequisites

None.

### Attributes

None.

### Examples

```
CNCRP;
```

### Output Format

```
MTP route configuration
ROUTE  NC   DPC       LS1  LS2  UPMASK   FLAGS
1      0    1         0    0    0x00020  0x00000
2      0    2         1    0    0x00020  0x00000
EXECUTED
```

## 6.9.5 CNCSP – Configuration Concerned Subsystem Print

### Synopsis

This command displays the concerned resources configuration. See Section 8.8.7, “SCCP_CONC_SSR” on page 165 for descriptions of the parameters in the output format.

### Syntax

```
CNCSP:[ID=],[CSSR=];
```

### Prerequisites

None.

### Attributes

None.

### Examples

```
CNCSP:ID=1;
```

### Output Format

```
Concerned Resource configuration
ID    NC CSSR CSPC     CSSN SSR SPC      SSN
4     1  RSP  1            LSS          8
5     1  LSS           8    RSP 3
6     1  LSS           8    RSS 1        8
EXECUTED
```

## 6.9.6 CNGAP – Configuration GTT Address Print

### Synopsis

This command is used to display currently configured SCCP Global Title Translation Addresses. The translations themselves are initially added statically via the configuration file config.txt. See Section 8.8.4, “SCCP_GTT_ADDRESS” on page 159 for further information relating to GTT address configuration.

### Syntax

```
CNGAP[[:ID=]|[:NC=]];
```

### Example

```
CNGAP;
GTT Address
  ID    NC    AI      SPC      SSN     GT                    GTAI_REPLACEMENT
  4      0    0x11    4369      0      0x001104              333/---/4
  5      0    0x11    17476     0      0x001104              55/
  1023   1    0x11    21845     0      0x001104              00/
EXECUTED
```

## 6.9.7 CNGLP – Configuration SIGTRAN Gateway List

### Synopsis

This command displays the configuration of relationships between Signaling Gateways and SIGTRAN Routes on the system.

### Syntax

```
CNGLP;
```

### Prerequisites

None.

### Attributes

None.

### Example

```
CNGLP;
```

### Output Format

```
Configuration SIGTRAN Gateway List
LIST SNRT  RSG
1    1     1
2    1     2
3    2     2
4    3     1
EXECUTED
```

### 6.9.8 CNGPP – Configuration GTT Pattern Print

#### Synopsis

This command is used to display currently configured SCCP Global Title Translation Patterns. The translations themselves are initially added statically via the configuration file config.txt. See Section 8.8.5, “SCCP_GTT_PATTERN” on page 161 for more information relation to the configuration of GTT patterns.

#### Syntax

```
CNGPP[[:ID=]|[:NC=]];
```

#### Example

```
CNGPP;
GTT Pattern
  ID    NC    AI      SPC      SSN     GT                      GTAI_PATTERN
  5      0    0x10    0         0      0x001104                22/?6+
  1023   1    0x10    0         0      0x001104                --/+6
  EXECUTED
```

### 6.9.9 CNGTP – Configuration Global Title Translation Print

#### Synopsis

This command is used to display currently configured SCCP Global Title Translation rules. The translations themselves are initially added statically via the configuration file config.txt. See Section 8.8.3, “SCCP_GTT” on page 158 for further inforatyion relating to GTT configuration.

#### Syntax

```
CNGTP[[:ID=]|[:NC=]];
```

#### Example

```
<cngtp;
  ID    NC     MASK                    PRI_ADDR_ID   BKUP_ADDR_ID
  4      0     R--/K--/R               4
  5      0     R-/K                    5
  1023   1     R-/K                    1023
EXECUTED
```

### 6.9.10 CNLSP – Configuration MTP Linkset Print

#### Synopsis

This command displays the current MTP linkset configuration. See Section , “MTP Link Set” on page 141 for descriptions of the parameters in the output format.

#### Syntax

```
CNLSP:[ID=];
```

#### Prerequisites

None.

#### Attributes

None.

#### Examples

```
CNLSP;
```

#### Output Format

Linkset configuration

```
LS  NC  OPC       APC       NLINKS  SSF  FLAGS
1   0   1         2         16      8    0x00003
2   0   1         3         16      8    0x00003
```

### 6.9.11 CNMLP – Configuration Monitor Link Print

#### Synopsis

This command displays the current Monitor link configuration. See Section 8.6.9, “MONITOR_LINK” on page 149 for descriptions of the parameters in the output format.

#### Syntax

```
CNMLP:[ID=];
```

#### Prerequisites

None.

#### Attributes

None.

#### Examples

```
CNMLP;
```

#### Output Format

```
Monitor link configuration
LINK IFTYPE    BPOS BLINK BPOS2 STREAM TS USER ID USER HOST FLAGS
0    TDM       3    1     3     0      16 0x0d    0         0x400210
1    TDM       3    2     3     1      16 0x0d    1         0x400210
EXECUTED
```

### 6.9.12 CNOBP – Display TRAP Configuration

#### Synopsis

This command displays the current TRAP configuration. The entire TRAP configuration for all available objects will be displayed, if no object group is specified. The list of available objects will depend on the current system mode configuration (i.e., SWS, SIU or SGW). If the objgrp parameter is specified, CNOBP will display settings for only that object group. The CNOBS command allows the TRAP configuration to be changed.

#### Syntax

```
CNOBP[:OBJGRP=];
```

#### Prerequisites

The DSMI-based SNMP agent must be enabled.

#### Attributes

None.

#### Examples

```
CNOBP;
CNOBP:OBJGRP=3;
```

#### Output Format

```
Configuration SNMP Traps
OBJGRP OBJECT  UP       DOWN     INACTIVE IMPAIR   RESTART  QUIESCE  WARNING
1      1       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
1      2       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
1      3       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
2      1       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
2      2       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
```

```
2       3       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
2       4       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
3       1       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
3       2       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
3       3       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
3       4       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
3       5       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
4       1       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
5       1       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
5       2       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
6       1       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
6       2       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
6       3       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
7       1       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
7       2       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
7       3       CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE   CHANGE
EXECUTED
```

### 6.9.13 CNOBS – Set TRAP Configuration

#### Synopsis

This command allows a user to determine the conditions under which an SNMP TRAP will be generated for a particular DSMI object.

Essentially, a TRAP can be generated:

- "When any row within an object changes state (CHANGE)
- "When a new row (with a particular state) is created within an object (CREATE)
- "When a row (with a particular state) is destroyed within an object (DESTROY)
- "When any combination of the above occur (ALL), or when an event occurs that affects the alarm condition of the object, but does not necessarily change the state.

TRAPs can also be completely disabled (NONE).

Possible states that a DSMI object can transition into are:

| | |
|---|---|
| UP | Operational and available |
| DOWN | Not available |
| INACTIVE | Operational but not available |
| IMPAIR | Operational and available but encountering service-affecting condition (e.g., congestion). |
| RESTART | Unavailable but will soon be available |
| QUIESCE | Operational but in the process of shutting down/being removed |
| WARNING | Operational and available but encountering a non service-affecting condition |

Only one state's TRAP configuration can be configured per single invocation of this command.

The CNOBP command displays the current TRAP configuration for each object.

These TRAP messages are sent to SNMP managers, which are defined with the CNSMI command. The default setting for object states is CHANGE.

#### Syntax

```
CNOBS:OBJGRP=,OBJECT=[,UP=]|[,DOWN=]|[,INACTIVE=]|[,IMPAIR=]|[,RESTART=]|[,QUIESCE=,]|[,WARNING=];
```

#### Prerequisites

The DSMI-based SNMP agent must be enabled.

#### Attributes

CONFIG

#### Examples

CNOBS:OBJGRP=7,OBJECT=2,DOWN=all;

This will cause a TRAP to be generated whenever an SS7 link is created in the Down state, or destroyed while in the Down state or when the link enters the Down state.

### 6.9.14 CNPCP – Configuration PCM Print

#### Synopsis

This command displays the current Monitor link configuration. See Section 8.5.2, “LIU_CONFIG” on page 133 for descriptions of the parameters in the output format.

#### Syntax

```
CNPCP;
```

#### Prerequisites

None.

Attributes

None.

#### Examples

```
CNPCP;
```

#### Output Format

```
PCM configuration
PORTID PCM LIUTYPE LC FF CRC SYNCPRI BUILDOUT SLAVE FLAGS
5      3-1 6       1  1  1   1       0         0     0x00000
6      3-2 6       1  1  1   1       0         0     0x00000
EXECUTED
```

### 6.9.15 CNRDI – Configuration Restore Defaults Initiate

#### Synopsis

This command is used to restore the protocol configuration file (config.txt) to the default version of the file, which does not include any commands, but provides guidelines on how to edit the file for a real configuration.

#### Syntax

```
CNRDI;
```

#### Prerequisites

None.

#### Attributes

CONFIG - The command affects configuration data.

#### Example

```
CNRDI;
```

### 6.9.16 CNSLP – Configuration SS7 Link Print

#### Synopsis

This command displays the current MTP signaling link configuration. See Section 8.6.4, “MTP_LINK” on page 142 for descriptions of the parameters in the output format.

#### Syntax

```
CNSLP:[ID=];
```

#### Prerequisites

None.

#### Attributes

None.

#### Examples

```
CNSLP;
```

#### Output Format

```
SS7 link configuration
LINK LINKSET LINKREF SLC BPOS BLINK BPOS2 STREAM TS FLAGS  IFTYPE
0    1       0       0   1    0     1     0      1  0x00006 TDM
1    1       1       1   1    1     1     0      2  0x00006 TDM
2    1       2       2   1    2     1     0      3  0x00006 TDM
3    1       3       3   1    3     1     0      4  0x00006 TDM
4    1       4       4   1    4     1     0      5  0x00006 TDM
5    1       5       5   1    5     1     0      6  0x00006 TDM
6    1       6       6   1    6     1     0      7  0x00006 TDM
7    1       7       7   1    7     1     0      8  0x00006 TDM
8    1       8       8   1    8     1     0      9  0x00006 TDM
9    1       9       9   1    9     1     0      10 0x00006 TDM
10   1       10      10  1    10    1     0      11 0x00006 TDM
11   1       11      11  1    11    1     0      12 0x00006 TDM
12   1       12      12  1    12    1     0      13 0x00006 TDM
13   1       13      13  1    13    1     0      14 0x00006 TDM
14   1       14      14  1    14    1     0      15 0x00006 TDM
15   1       15      15  1    15    1     0      16 0x00006 TDM
16   2       0       0   1    16    1     0      17 0x00006 TDM
EXECUTED
```

### 6.9.17 CNSMC – Change SNMP Manager Configuration

#### Synopsis

This command allows the administrator to alter an SNMP manager's configuration. The parameters and the associated values are as per the CNSMI command.

#### Syntax

```
CNSMC:MNGR={,IPADDR=|,TFORMAT=|,PORT=|,TCOM=|,USER=|,ENGINE=|,LABEL=};
```

#### Prerequisites

The DSMI-based SNMP agent must be enabled.

The manager must already have been defined with the CNSMI command.

If an SNMP v3 user is specified, the user must already be defined.

#### Attributes

CONFIG

### Examples

```
CNSMC:MNGR=1,IPADDR=192.168.220.222;
```

## 6.9.18 CNSME – End SNMP Manager Configuration

### Synopsis

This command removes an SNMP manager definition from the list of configured SNMP managers. The command takes a single parameter, MNGR, which identifies the particular manage to remove.

### Syntax

```
CNSME:MNGR=;
```

### Prerequisites

The DSMI-based SNMP agent must be enabled.

The manager must already have been defined with the CNSMI command.

### Attributes

CONFIG

### Examples

```
CNSME:MNGR=1;
```

## 6.9.19 CNSMI – Set SNMP Manager Configuration

### Synopsis

This command allows the administrator to define up to 32 TRAP destinations (i.e., remote SNMP manager stations). Each manager is defined by its IP address (IPADDR). Additionally, the type of TRAP to be dispatched to the SNMP manager is specified with the TFORMAT parameter. The following values are supported:

| | |
|---|---|
| 1 | An SNMP v1 TRAP is sent |
| 2 | An SNMP v2 TRAP is sent |
| 3 | An SNMP v2 INFORM is sent |

The PORT parameter allows you to configure a destination port which is different from the default standard SNMP TRAP port (162).

If the remote SNMP (v1 or v2c) manager has been configured to only recognize TRAPs received with a community string, the TCOM parameter accommodates that value.

If an SNMP v3 TRAP is to be issued, then the USER parameter value is used. The USER parameter is used to specify a user, which has been defined with the CNUSI command. Furthermore, it will also be necessary to configure an engine identifier, which has been configured on the remote SNMP manager. The engine identifier is configured with the ENGINE parameter.

Finally, the LABEL parameter is used to specify an optional string identifier for the manager.

### Syntax

```
CNSMI:MNGR=,IPADDR=,TFORMAT=[,PORT=][,TCOM=][,USER=][,ENGINE=][,LABEL=];
```

### Prerequisites

The DSMI-based SNMP agent must be enabled. If an SNMP v3 TRAP is required, the user referenced by the USER parameter must exist.

#### Attributes

CONFIG

#### Examples

This is an example for setting up a simple SNMP v2 TRAP receiver/manager:

```
CNSMI:MNGR=1,IPADDR=192.168.1.22,TFORMAT=2;
```

This next example shows how an SNMP v3 TRAP receiver/manager would be created. The first step is to define the user with the CNUSI command:

```
CNUSI:USER=1,AUTH=MD5,AUTHPASS=abcdefgh,LABEL=user1;
EXECUTED
```

The next step is to define the manager which references the user which has just been defined:

```
CNSMI:MNGR=2,IPADDR=192.168.1.222,USER=1,ENGINE=1122334455;
EXECUTED
```

### 6.9.20 CNSMP – Display SNMP Manager Configuration

#### Synopsis

This command displays the currently configured SNMP managers. If a MNGR value is specified, only that manager is displayed.

#### Syntax

```
CNSMP [:MNGR=];
```

#### Prerequisites

The DSMI-based SNMP agent must be enabled.

#### Attributes

None.

#### Examples

```
CNSMP;
```

#### Output Format

```
Configuration SNMP Manager
MNGR  IPADDR           PORT TFORMAT TCOM      USER  ENGINEID  LABEL
1     192.168.220.192   162  1                  0
EXECUTED
```

### 6.9.21 CNSNP – Configuration SNMP Print

#### Synopsis

This command displays the current SNMP mode, including the read and, where applicable, the write community string. The current SNMP agent, however, does not support write access. The output of this command can be used to determine which, if any, SNMP agent is currently activated on the Server. In the case of the enhanced DSMI-based agent, the SNMP setting will be DSMI. In the case of the legacy SNMP support, the value is DK4032. Additionally, if SNMP is not currently activated, a value of NONE will be displayed.

#### Syntax

```
CNSNP;
```

#### Prerequisites

None

#### Attributes

None

#### Example

```
CNSNP;
```

#### Output Format

```
SNMP Configuration
SNMP DSMI
RCOM ********
WCOM ********
EXECUTED
```

### 6.9.22 CNSNS – Configuration SNMP Set

#### Synopsis

This command is used to select an SNMP agent or to disable SNMP. Changing the SNMP parameter with the CNSNS command will require a system restart for the changes to take effect. The SNMP parameter value can be one of three values. Setting the SNMP value to DK4032 will activate the legacy SNMP support. Setting the SNMP value to DSMI will activate the enhanced, DSMI-based agent if there is a valid license on the server. Finally, SNMP can be disabled altogether by specifying a value of NONE.

***Note:*** When the DSMI-based SNMP agent is enabled initially, the RCOM string is assigned a value of "public" and the WCOM string a value of "private". Unlike the legacy SNMP agent (SNMP=DK4032), there is no support for SNMP requests without a community string.

#### Syntax

```
CNSNS:SNMP=,[RCOM=,CONFIRM=],[WCOM=,CONFIRM=];
```

#### Prerequisites

Before DSMI SNMP functionality can be activated, the unit must be equipped with the SNMP license.

#### Example

```
CNSNS:SNMP=DSMI,RCOM=rcomstring,CONFIRM=rcomstring;
```

### 6.9.23 CNSRP – Configuration SIGTRAN Route Print

#### Synopsis

This command displays the configuration of SIGTRAN Routes on the system.

#### Syntax

```
CNSRP;
```

#### Prerequisites

None

#### Attributes

None

#### Example

```
CNSRP;
```

### Output Format

```
Configuration SIGTRAN Routes
SNRT  NC  DPC       OPTIONS
1     1   664       0x0002
2     1   56444     0x0002
3     1   3334      0x0002
EXECUTED
```

### 6.9.24 CNSTP – Configuration SIGTRAN Links Print

#### Synopsis

This command displays the configuration of Sigtran links.

#### Syntax

CNSTP:[SNLINK=,][TYPE=][PAGE=];

#### Prerequisites

None

#### Example

CNSTP;

#### Output format

```
SIGTRAN Link Configuration (Page 1 of 2)
SNLINK  TYPE  LIP1            RIP1            LIP2            RIP2
1       M3UA  10.22.131.1     10.22.131.2
EXECUTED

SIGTRAN Link Configuration (Page 2 of 2)
SNLINK  TYPE  END LPORT RPORT FLAGS  M2PA ID RSG NC   NA
1       M3UA  C   3565 3565   0x0000             0
EXECUTED
```

The meaning of each field in the output is as follows:

- SNLINK - The SIGTRAN link identifier.
- TYPE - The type of link (M2PA M3UA).
- LIP1 - The first local IP address in the association.
- RIP1 - The first remote IP address in the association.
- LIP2 - The second local IP address in the association.
- RIP2 - The second remote IP address in the association.
- END - Client or Server.
- LPORT - Local IP port for the association.
- RPORT - Remote IP port for the association.
- FLAGS - Flags associated with the SIGTRAN link.
- M2PAID - M2PA Identifier (M2PA only.
- RSG - Remote Signaling Gateway (M3UA only).
- NC - Network Context (M3UA only).
- NA - Network Appearance (M3UA only).

### 6.9.25 CNSSP – Configuration Subsystem Resource Print

#### Synopsis

This command displays the SCCP subsystem resource configuration. See Section 8.8.6, “SCCP_SSR” on page 162 for descriptions of the parameters in the output format.

#### Syntax

CNSSP:[ID=],[SSR={LSS|RSS|RSP}];

### Prerequisites

None.

### Attributes

None.

### Examples

```
CNSSP:ID=2;
```

### Output Format

```
Subsystem configuration
ID     NC SSR SPC       SSN MODULE FLAGS  PCMASK     PROT
0      0  LSS           12  0x000d 0x0000             DTS
1      0  RSP 1                    0x0000 0x00000000
2      0  RSS 1         12         0x0000
EXECUTED
```

## 6.9.26 CNSWP – Configuration Software Print

### Synopsis

For the current operating mode, the command on the first page displays the software operating on the main CPU and signaling boards within the Signaling Server. On this page, the command also displays the library version numbers for each protocol configured on the unit.

The second page of the CNSWP command displays the software available for other modes operation.

### Syntax

```
CNSWP: [PAGE=,]
```

### Prerequisites

None.

### Attributes

None.

### Example

```
CNSWP;
```

### Output Format

```
Software Configuration (Page 1 of 2)
SS7G30-SWS Release 2.2.0 (Build 1004)
Dialogic(R) DSI Signaling Server - SWS Mode
Copyright (C) Dialogic Corporation 1994-2010
Protocol Libraries
MTP3 CPU     V6.10
M2PA CPU     V1.14
EXECUTED

cnswp:page=2;
SS7G31(SWS) Software Configuration (Page 2 of 2)
MODE STATUS      VERSION
SWS  Available   SS7G30-SWS Release 2.2.0 (Build 1004)
SGW  Available   Release prior to 2.2.0
EXECUTED
```

### 6.9.27 CNSYP – Configuration System Print

#### Synopsis

This command is used to print the system configuration, including the system contact and system location details. The configuration items include the unit identity (UNIT ID), mode (SIUA or SIUB) and protocol options. Protocol module options not licensed on the unit do not appear in the list. Most of these configuration items are set using the CNSYS command, which also contains more details of other options.

#### Syntax

```
CNSYP: [PAGE=,]
```

#### Prerequisites

None.

#### Attributes

None.

#### Example

```
CNSYP;
```

#### Output Format

```
SS7G30(SWS) System Configuration (Page 1 of 2)
UNITID000423a684d1
SYSID
SYSREF0
CONTACT EMAIL@EXAMPLE.COM
LOCATION RACK3
FTPSER      Y
MODE        SIUA
SECURE      N
LEDID       N
TRACELOG    FILE
TRACEFMT    TEXT
DMHOST      0
SN1
EXECUTED

SS7G30(SWS) System Configuration (Page 2 of 2)

SCCPCL  Y
SCCPCO  Y
TCAP    Y
MAP     Y
EXECUTED
```

### 6.9.28 CNSYS – Configuration System Set

#### Synopsis

This command is used to activate protocol options, and set the system, level parameters and passwords.

When FTPSER is enabled, the unit acts like an FTP server supporting the upload of configuration files, software upgrade and purchasable licenses from a remote unit. To maintain security, it is recommended that FTPSER is disabled at all times when FTP services are not required. You can allow FTP access to the SWS by using the FTPSER parameter. You can disable FTPSER by setting the parameter to N. Activation and deactivation of the FTP server takes immediate effect.

You can restrict access to the SWS so that it operates only over secure shell (SSH) by using the SECURE parameter. By default, there is no restriction allowing the use of normal telnet and FTP. You can enable secure operation by setting the SECURE parameter to Y. Activation and deactivation of secure operation takes immediate effect.

The MODE parameter is used to select the operating mode of the unit. A unit that is operating as a standalone unit should be operated in SIUA mode. When two units are used in a dual resilient configuration, one unit should operate in SIUA mode and the other should operate in SIUB mode.

Changes to the MODE parameter value require a system restart in order to take effect. Activation of protocols require a system restart.

You can set system location and system contact details. These values will be mirrored in the System Data object of the System group (i.e., DSMI-SYSTEM-OBJECTS-MIB::systemDataObjectTable).

When a password is specified, all new MML sessions, except for serial port 2 (COM2), require the password before entry.

### Syntax

```
CNSYS: {[SYSID=,] [SYSREF=,] [MODE=,][SECURE=,] [LEDID=,] [TRACELOG=,][TRACEFMT=][DMHOST=,]
[FTPPWD=,][FTPSER=,] [SCCPCL=,] [SCCPCO=,] [TCAP=,]
[MAP=,]};
CNSYS:[LOCATION=|ICONTACT=I];
CNSYS:PASSWORD=,CONFIRM=
```

### Prerequisites

The following restrictions apply:

- A higher layer protocol might not be enabled if the lower layer it is dependant on is not enabled (for example, INAP might not be enabled if TCAP and SCCPCL or SCCPCO are not enabled).
- A lower layer protocol might not be disabled if there is an enabled higher layer protocol dependant on it (for example, TCAP might not be disabled if MAP is enabled).

### Attributes

CONFIG - The command affects configuration data.

### Examples

```
CNSYS:MODE=SIUB;
CNSYS:MAP=Y;
CNSYS:LOCATION=RACK3,CONTACT=ADMIN@MAIL.COM;
```

### 6.9.29 CNTDP – Configuration Time and Date Print

#### Synopsis

This command is used to print out the system date and time, whether NTP is active and to display the OFFSET from UTC configured. See the CNTDS command for setting the time and date, UTC OFFSET and activating NTP.

#### Syntax

```
CNTDP;
```

#### Prerequisites

None.

#### Attributes

None.

#### Example

```
CNTDP;
Configuration Time and Date
DATE       TIME     NTP OFFSET
2001-10-03 09:04:02 Y -5:30
```

### 6.9.30 CNTDS – Configuration Time and Date Set

#### Synopsis

This command is used to specify the date (DATE) and time (TIME) as used by the system. This command can also activate or deactivate Network Time Protocol (NTP) on the system. System time is used by the Signaling Server to indicate the time an alarm occurred or cleared and to provide timestamps for such things as measurements and data records. The command also allows an OFFSET from UTC to be specified to allow the system to report the correct local time, when synchronized with an NTP time server.

***Note:*** The system will not automatically adjust for daylight savings time changes.

See:

- The CNTDP command to verify the time and date settings.
- The CNTPI command to add NTP servers to the configuration.
- The STTPP command to view the current NTP server status.

***Note:*** The current system time must be within 1000 seconds (just over 15 minutes) of the time currently used by an active NTP server for NTP time synchronization to be successful. If the time is not within that range, then NTP synchronization will fail, the STTPP command will indicate that the NTP servers are INACTIVE, and the system will continue to use its current time. In this event, if the user wishes to use time based on that used by the NTP servers, then the user should modify system time using CNTDS to be within 1000 seconds after which the signaling server will automatically re-attempt synchronization.

#### Syntax

```
CNTDS:[DATE=,][TIME=,][NTP=,][OFFSET=];
```

#### Prerequisites

The OFFSET value must be specified in hours and optionally 0 or 30 minutes, in the range -14 to +12. The OFFSET is specified in POSIX-style, which has positive signs west of Greenwich. e.g.,

| | |
|---|---|
| Montreal, CANADA | +5:00 |
| Parsippany, USA | +5:00 |

| | |
|---|---|
| Fordingbridge, UNITED KINGDOM | 0:00 |
| Renningen, GERMANY | -1:00 |
| New Delhi, INDIA | -5:30 |
| Beijing, CHINA | -8:00 |
| Sydney, AUSTRALIA | -10:00 |

The unit must be restarted in order for the new OFFSET value to take effect.

#### Attributes

CONFIG - The command affects configuration data.

#### Example

```
CNTDS:DATE=2001-10-03,TIME=18:32:21,NTP=Y,OFFSET=-5:30;
EXECUTED
```

### 6.9.31 CNTMP – Configuration Trace Mask Print

#### Synopsis

This command is used to print the current trace masks and whether or not tracing is enabled.

#### Syntax

```
CNTMP;
```

#### Prerequisites

None.

#### Attributes

None.

#### Example

```
CNTMP;
```

#### Output Format

```
<CNTMP;
Trace Masks Configuration
MODULE      IMASK         OMASK         MMASK      ACTIVE
MTP         0x00030000    0x0003c001    0x0001fffe   Y
TCAP        0x00000003    0x00000003    0x00000000   N
MAP         0x00000003    0x00000003    0x00000014   N
SCCP        0x00000003    0x00000003    0x00000001   N
M3UA        0x00000000    0x00000000    0x00000000   N
EXECUTED
```

Definitions of the trace mask parameters, IMASK, OMASK and MMASK, for a specific protocol are documented in the associated protocol Programmer's Manual.

### 6.9.32 CNTMS – Configuration Trace Mask Set

#### Synopsis

This command is used to activate or deactivate tracing of different protocols and to set the associated trace masks. Configured values are maintained after system reset. The IMASK, OMASK, and MMASK parameters determine which Input, Output or Management messages are traced by the module. Default IMASK, OMASK, or MMASK values may be restored using the 'DEFAULT' token.

***Note:*** Definitions of the IMASK, OMASK and MMASK trace mask parameters, for a specific protocol are documented in the associated protocol Programmer's Manual.

By default, when tracing is activated on the SWS, messages are logged to file in the 'syslog' subdirectory of the siuftp account. This log is maintained as a rolling log of up to 10 5MB files containing trace messages. The most recent trace log file will have the name trace.log' the next most recent trace.log.1' and then trace.log.2' and so on.

A user may change the destination of trace messages through use of the TRACELOG parameter on the CNSYx command. A user also can select either that messages a logged to FILE (default), HOST, where they are transmitted to the management module id on the configured management host, or DUAL where they are both logged to file and sent to host.

MTP3 and M3UA traces may also be logged in PCAP file format. In a similar manner to the above text log files, the system supports up to 10, 5MB PCAP log file named trace.pcap, trace.pcap.1, trace.pcap.2 etc. storing them in the syslog subdirectory of the siuftp account. Logging in TEXT or PCAP format is selected by using the TRACEFMT parameter in the CNSYx MMI command.

Activation of tracing under high load conditions may reduce overall throughput of the SWS. For systems operating under relatively light traffic conditions, permanent activation of tracing to file at an MTP layer may be considered beneficial for maintenance purposes.

When tracing, users should consider the confidential aspects of maintaining a log of message data. Trace, as well as other diagnostic data, can be removed from the "syslog" subdirectory by performing a soft restart of the system using the following MMI command:

```
MNRSI:RESTART=SOFT,RESET=Y;
```

### Syntax

```
CNTMS:MODULE={[IMASK=,][OMASK=,][MMASK=,][ACTIVE=]};
```

### Prerequisites

The protocol should be licensed and active before attempting to configure a trace mask for it.

### Attributes

CONFIG - The command affects configuration data.

### Examples

```
CNTMS:MODULE=MAP,IMASK=1,OMASK=2,MMASK=3;
CNTMS:MODULE=MAP,ACTIVE=Y;
CNTMS:MODULE=MAP,ACTIVE=N;
CNTMS:MODULE=MAP,IMASK=DEFAULT;
```

***Note:*** This command causes a copy of selected protocol messages to be taken and sent to destination module 0xef on host_id 0 facilitating the examination of raw SS7 parameters for diagnostic purposes. The traced message is formatted in accordance with the specification of the MGT_MSG_TRACE_EV message described in Chapter 10, "Application Programming Interface".

### 6.9.33 CNTPE – Configuration Network Time Protocol Server End

#### Synopsis

This command is used to remove an NTP Server from the configuration of the system.

#### Syntax

```
CNTPE:NTPSER;
```

#### Prerequisites

The specified NTPSER must already be configured.

#### Attributes

CONFIG - The command affects configuration data.

#### Example

```
CNTPE:NTPSER=1;
```

### 6.9.34 CNTPI – Configuration Network Time Protocol Server Initiate

#### Synopsis

This command is used to add an NTP server to the configuration of the system. The NTP service should be activated using the CNTDS command.

#### Syntax

```
CNTPI:NTPSER=,IPADDR=,[LABEL=];
```

#### Prerequisites

The specified NTPSER must not already be configured.

The IPADDR might not be used more than once and might not identify any of the configured system IP addresses.

Up to 16 NTP servers may be configured.

#### Attributes

CONFIG - The command affects configuration data.

#### Example

```
CNTPI:NTPSER=1,IPADDR=192.168.0.1,LABEL=NTPSERV1;
```

### 6.9.35 CNTPP – Configuration Network Time Protocol Print

#### Synopsis

This command is used to display the configuration of the Network Time Protocol software on the unit.

#### Syntax

```
CNTPP;
```

#### Prerequisites

None.

#### Attributes

None.

### Example

```
CNTPP;
Configuration of NTP Servers
NTPSER IPADDR          LABEL
1      192.168.0.1     NTP server 1
2      192.168.0.2     NTP server 2
EXECUTED
```

### 6.9.36 CNUAP – Configuration User Account Print

#### Synopsis

Displays the characteristics of a user account.

If a non default password is present, it will be displayed as "********".

If no password is present for the admin account, then it will be displayed as blank.

If the siuftp account has been set to null while a null string is displayed, the user will be expected to enter the default 'siuftp' password for the siuftp account.

#### Syntax

CNUAP;

#### Prerequisites

None

#### Attributes

None

#### Examples

CNUAP;

#### Output Format

```
User Account Characteristics
USER     PASSWORD
admin    ********
siuftp
EXECUTED
```

### 6.9.37 CNUAS – Configuration User Account Set

#### Synopsis

Configures the characteristics of a user account.

If a null password is entered for the admin account, then no password will be required for MMI access.

If a null password is entered for siuftp, the password will be set to the default password "siuftp" for the account.

#### Syntax

CNUAS:USER=admin, PASSWORD=, CONFIRM=;

CNUAS:USER=siuftp, PASSWORD=, CONFIRM=;

#### Prerequisites

The following restrictions apply:

- If a PASSWORD is entered, then the CONFIRM parameter is required. The character strings for these two parameters must be equal.

The password used, apart from the NULL password must:

Not have been one of the past 8 passwords used

Be minimum of 8 characters and a maximum of 15 characters.

Have 1 Upper case character, 1 Lower Case character, 1 Digit and 1 special character.Special characters supported are:

~ % ^ @ $ #

**Attributes**

None

**Examples**

```
CNUAS:USER=admin,PASSWORD=Di@l0gic,CONFIRM= Di@l0gic;
CNUAS:USER=admin,PASSWORD=,CONFIRM=;
```

### 6.9.38 CNUPI – Configuration Update Initiate

**Synopsis**

This command is used to validate that a license file transferred to portable media has been created without error.

The command will return EXECUTED if the license file on the portable media is without error.

**Syntax**

```
CNUPI:DTYPE=;
```

**Example**

```
CNUPI:DTYPE=SYSKEY;
```

### 6.9.39 CNURC – Configuration Update Resource Change

**Synopsis**

This command is used to change the configuration of a resource and update the configuration data on the SWS. The operation involves reading the config.txt file containing configuration data, validating it, and applying it to the unit. The command can be applied to circuit groups (mode=CGRP), MTP linksets (mode=MTPLS) and MTP routes (mode=MTPR).

On an MTP linkset, only the num_links parameter can be changed. On an MTP route, only the linkset_id, 2nd linkset_id and flags parameters may be changed. See Section 9.7.1, “Config.txt-Based Dynamic Configuration” on page 173 for more information.

**Syntax**

```
CNURC:MODE=,ID=;
```

**Prerequisites**

The command succeeds only if the resource specified by the ID parameter is present in the updated configuration file and a valid configuration has been entered.

All links in the linkset must be deactivated before linksets can be changed.

Any linkset identified by the MTP_ROUTE command must already be configured.

**Attributes**

CONFIG - The command affects configuration data.

**Example**

```
CNURC:MODE=CGRP,ID=2;
CNURC:MODE=MTPR,ID=1;
CNURC:MODE=MTPLS,ID=11;
```

### 6.9.40 CNURE – Configuration Update Resource End

#### Synopsis

This command is used to end the configuration of a resource and update the configuration data on the SWS. The operation involves reading the config.txt file containing configuration data, validating it, and applying it to the unit. The command can be applied to circuit groups (mode=CGRP), MTP linksets (mode=MTPLS), MTP links (mode=MTPL), MTP routes (mode=MTPR), Monitoring links (mode=MONL), and PCM (mode=LIU). See Section 9.7.1, “Config.txt-Based Dynamic Configuration” on page 173 for more information.

#### Syntax

```
CNURE:MODE=,ID=;
```

#### Prerequisites

The command succeeds only if the resource specified by the ID parameter not present in the updated configuration file, the specified resource was previously configured and is in an INACTIVE state.

When removing MTP links, the links must first be deactivated. If a link is to be removed from an SPCI4 signaling board, the board must be reset (RSBOI) following the execution of this command.

An MTP linkset cannot be removed if it contains MTP links or is used on any MTP route.

#### Attributes

CONFIG - The command affects configuration data.

#### Example

```
CNURE:MODE=CGRP,ID=8;
```

### 6.9.41 CNURI – Configuration Update Resource Initiate

#### Synopsis

This command is used to add a new resource to the configuration of the unit and update the configuration data on the SWS. The operation involves reading the config.txt file containing configuration data, validating it and applying it to the unit. The modes that can be used to initiate new resources are: CGRP, MTPR, MTPLS, MTPL, MONL, LIU, SSR, CSSR, M3UAR or M3UARLIST. See Section 9.7.1, “Config.txt-Based Dynamic Configuration” on page 173 for more information.

***Note:*** Adding an MTP route to an adjacent Signaling End Point (SEP) will require any/all previously configured MTP links associated with the route to be taken out of service using MNINI and then brought back into service using MNINE to allow the route to come fully into service. New MTP routes that reach a destination via an STP do not require this additional step and will come into service on the completion of the Signaling Route Set Test mechanism.

#### Syntax

```
CNURI:MODE=,ID=;
```

#### Prerequisites

The command succeeds only if the resource specified by the ID parameter is present in the updated configuration file, a valid configuration has been entered and the specified resource was not previously configured on the unit.

When adding links to an SPCI4 signaling board, the board must be reset (RSBOI) following the execution of this command and after reset the link must be activated using MNINE.

#### Attributes

CONFIG - The command affects configuration data.

### Example

```
CNURI:MODE=MTPR,ID=5;
CNURI:MODE=SSR,ID=8;
CNURI:MODE=M3UAR,ID=2;
CNURI:MODE=M3UARLIST,ID=33;
```

## 6.9.42 CNUSC – Change SNMP v3 User Configuration

### Synopsis

This command allows the configuration of a previously registered SNMP v3 user to be changed. The USER parameter identifies the user account to modify.

The parameters and associated values are as per the CNUSI command, with the additional parameters PRIV and PRIVPASS. Supported PRIV parameter values are DES and AES. As with the AUTHPASS parameter value, the privacy password value (PRIVPASS) must be between 8 and 24 characters long. Also, it is not possible to configure or modify the PRIVPASS value for a user without also specifying the PRIV value. It is, however, possible to modify the PRIV or AUTH values without additionally specifying a corresponding password.

### Syntax

```
CNUSC:USER=[,AUTH=|,AUTHPASS=|,PRIV=|,PRIVPASS=|,LABEL=};
```

### Prerequisites

The DSMI-based SNMP agent must be enabled.

The SNMP v3 user must already have an entry in the list of configured SNMP v3 users.

### Attributes

CONFIG

### Examples

```
CNUSC:USER=3,AUTH=SHA;
```

## 6.9.43 CNUSE – End SNMP v3

### Synopsis

This command removes an SNMP v3 user's configuration entry. The command takes a single parameter, USER, which identifies the user to be removed.

### Syntax

```
CNUSE:USER=;
```

### Prerequisites

The DSMI-based SNMP agent must be enabled.

The user must be present in the list of configured SNMP v3 users.

### Attributes

CONFIG

### Examples

```
CNUSE:USER=3;
```

### 6.9.44 CNUSI – Set SNMP v3

#### Synopsis

This command allows the administrator to create SNMP v3 user accounts that are recognized by the local server. It also allows the administrator to define SNMP v3 user accounts for use in conjunction with SNMP v3 TRAP destinations/managers.

A user is defined with an integer user identifier (USER), optional authentication (AUTH/AUTHPASS) and a label (LABEL), which serves as the username. The USER and LABEL parameters are mandatory. Supported AUTH values are SHA and MD5. The password must have a minimum length of 8 characters, and a maximum length of 24 is enforced. The AUTH and AUTHPASS parameters must be specified together. In other words, it is not possible to configure an AUTHPASS value without having also specified the AUTH value.

Note that only the authentication attributes can be defined with the CNUSI command. If a user requires privacy (encryption) parameters to be applied, the CNUSC command is used to configure them.

#### Syntax

```
CNUSI:USER=[,AUTH=,AUTHPASS=],LABEL=;
```

#### Prerequisites

The DSMI-based SNMP agent must be enabled.

#### Attributes

CONFIG

#### Examples

```
CNUSI:USER=3,AUTH=MD5,AUTHPASS=user3pass,LABEL=user3;
```

### 6.9.45 CNUSP – Display SNMP v3

#### Synopsis

This command displays the current list of configured SNMP v3 users. The passwords are hidden. If a USER value is specified with the command, only that user's details are displayed.

#### Syntax

```
CNUSP[:USER=];
```

#### Prerequisites

The DSMI-based SNMP agent must be enabled.

#### Attributes

None.

#### Examples

```
CNUSP;
```

#### Output Format

```
Configuration SNMP Users
USER  AUTH  AUTHPASS  PRIV  PRIVPASS  LABEL
1     MD5   ********  NONE            user1
2     SHA   ********  NONE            user2
EXECUTED
```

## 6.10 IP Commands

The IP commands include:

- IPEPS - Set Ethernet Port Configuration
- IPEPP - Display Ethernet Port Configuration
- IPGWI - Internet Protocol Gateway Initiate
- IPGWE - Internet Protocol Gateway End
- IPGWP - Internet Protocol Gateway Print
- IPWSP - Display Web Service Configuration
- IPWSS -Web Service Configuration Set

### 6.10.1 IPEPS – Set Ethernet Port Configuration

#### Synopsis

This command is used to configure Ethernet ports.

The SWS supports resilient IP connectivity when you configure a team of two ports in an active/standby role. Three IP bonding teams can be created from the six ethernet ports available. A bonding team, assigned a single IP address, consists of a primary (active) port and a secondary (standby) port. The secondary port IP address should be set to one of the following values:

- STANDBY1 - The configured IP address acts as the standby port in a team with ETH1.
- STANDBY2 - The configured IP address acts as the standby port in a team with ETH2.
- STANDBY3 - The configured IP address acts as the standby port in a team with ETH3.
- STANDBY4 - The configured IP address acts as the standby port in a team with ETH4.
- STANDBY5 - The configured IP address acts as the standby port in a team with ETH5.
- STANDBY6 - The configured IP address acts as the standby port in a team with ETH6.

#### Syntax

```
IPEPS:ETH=, {[SPEED=,] [IPADDR=,][SUBNET=,] [SCTP=]};
```

#### Prerequisites

None.

#### Limitations

The use of the SCTP parameter has been deprecated. The system will ignore the setting of this parameter if per association hosts are specified. The parameter itself will continue to be supported to provide backwards compatibility with configurations that did not specify per association local IP addresses.

#### Attributes

CONFIG - The command affects configuration data.

#### Example 1

```
IPEPS:ETH=1,SPEED=100;
```

#### Example 2

```
IPEPS:ETH=2,IPADDR=192.168.0.1,SCTP=Y;
```

#### Example 3

```
IPEPS:ETH=3,IPADDR=10.1.1.10,SUBNET=255.255.1.1;
```

#### Example 4

```
IPEPS:ETH=4,IPADDR=STANDBY2;
```

### 6.10.2 IPEPP – Display Ethernet Port Configuration

#### Synopsis

This command displays the Ethernet port configuration. A Ethernet port speed displayed with an H indicates it is half-duplex, otherwise it is full-duplex.

#### Syntax

```
IPEPP;
```

#### Prerequisites

None

#### Attributes

None.

#### Example

```
IPEPP;
```

#### Output Format

```
<ipepp;
ETH SPEED IPADDR          SUBNET          SCTP MGMT WSAPI
1   AUTO  192.168.0.1     255.255.255.0   Y    Y    N
2   AUTO  10.100.91.3     255.255.255.0   Y    N    Y
3   AUTO  0.0.0.0         255.255.255.0   Y    Y    Y
4   AUTO  0.0.0.0         255.255.255.0   N    Y    Y
EXECUTED
```

### 6.10.3 IPWSP - Display Web Service Configuration

#### Synopsis

This command displays the configuration for web services.

#### Syntax

```
IPWSP;
```

#### Prerequisites

None

#### Attributes

None.

#### Example

```
IPWSP;
```

#### Output Format

```
<ipwsp;
WEBSERV HTTPPORT HTTPSPORT HTTPSCERT
MGMT    80       443       SELF
WSAPI   81
EXECUTED
```

### 6.10.4 IPWSS -Web Service Configuration Set

#### Synopsis

This command configures parameters for web services. It allows HTTP and HTTPS Port numbers and the type of Certificate for HTTPS to be specified. Supported SSL certificates for HTTPS are OpenSSL '.PEM' files, without a passphrase.

To load a certificate, the certificate file should be named either "MGMT.PEM" or "WSAPI.PEM" and uploaded to the siuftp account. This certificate will be installed and used when the system is restarted. The file will be removed from siuftp account once installed. Certificates may also be loaded via portable media.

#### Syntax

```
IPWSS:WEBSERV=[MGMT|WSAPI],{[HTTPPORT=,][HTTPSPORT=,][HTTPSCERT=,]};
```

#### Prerequisites

The following restrictions apply:

- The specified HTTPPORT or HTTPSPORT port might not be already used.
- When HTTPSCERT is set to FILE and no certificate is installed, the HTTPSCERT will revert to NONE.

#### Attributes

CONFIG - The command affects configuration data.

#### Example

```
IPWSS:WEBSERV=MGMT,HTTPPORT=0,HTTPSPORT=443;
```

#### Parameter Definitions:

WEBSERV

Specifies the type of Web Server to configure. Either MGMT or WSAPI.

HTTPPORT

The TCP Port used for HTTP. Set to 0 to disable access via HTTP. Valid Range 0:65,535 excluding 21, 22, 8100, 8101, 9000-9128, the value identified by HTTPSPORT or the HTTPPORT value of another WEBSERV.

HTTPSPORT

The TCP Port used for HTTPS. Set to 0 to disable access via HTTPS. Valid Range 0:65,535 excluding 21, 22, 8100, 8101, 9000-9128, the value identified by HTTPSPORT or the HTTPSPORT value of another WEBSERV.

HTTPSCERT

Identify the certificate to use for the WEBSERV. If set to FILE then the corresponding certificate will be used. If set to SELF, a new self-signed certificate will be generated and installed. If set to NONE the certificate for that web service will be removed.

Valid values are:

NONE
SELF
FILE

### 6.10.5 IPGWI – Internet Protocol Gateway Initiate

#### Synopsis

This command allows you to specify a route (IPGW) to an IP network (IPNW) via an IP gateway (GATEWAY) for a range of IP addresses within that network as defined by a network mask (MASK).

#### Syntax

```
IPGWI:IPGW=DEFAULT,GATEWAY=;
IPGWI:IPGW={1..31},MASK=,GATEWAY=,IPNW=;
```

#### Prerequisites

The IP gateway ID has not been initiated.

Two gateways cannot have overlapping IP addresses.

#### Attributes

CONFIG - The command affects configuration data.

#### Example 1

```
IPGWI:IPGW=1,MASK=255.255.255.0,GATEWAY=192.168.1.1,IPNW=172.16.1.0;
```

#### Example 2

```
IPGWI:IPGW=DEFAULT, GATEWAY=192.168.1.1;
```

### 6.10.6 IPGWE – Internet Protocol Gateway End

#### Synopsis

This command removes an IP route via an IP gateway.

#### Syntax

```
IPGWE:IPGW=;
```

#### Prerequisites

The IP gateway ID has been initiated.

#### Attributes

CONFIG - The command affects configuration data.

#### Example

```
IPGWI:IPGW=1;
```

### 6.10.7 IPGWP – Internet Protocol Gateway Print

#### Synopsis

This command prints out routes via IP gateways.

#### Syntax

```
IPGWP:[IPGW=,];
```

#### Prerequisites

If IPGW= is specified, the specified IP gateway ID (IPGW) must have been initiated.

#### Attributes

None.

#### Example

```
IPGW    GATEWAY         MASK              IPNW
DEFAULT 192.168.1.1
1       192.168.1.1     255.255.255.0     172.16.1.0
```

## 6.11 MML Commands

The MML commands include:

- MMLOI - MML Log Off Initiate
- MMHPP - MML Help Print

### 6.11.1 MMLOI – MML Log Off Initiate

#### Synopsis

This command ends the current log-on session and allows a new session to be used on the port. It does not affect other MML interface sessions.

#### Syntax

```
MMLOI;
```

#### Prerequisites

None.

#### Attributes

None.

#### Example

```
MMLOI;
```

### 6.11.2 MMHPP – MML Help Print

#### Synopsis

This command prints out help for MML commands, parameters and errors. When specified without parameters, the MMHPP command provides a list of commands.

#### Syntax

```
MMHPP:[CMD=,][CLASS=,];
```

#### Prerequisites

None.

#### Attributes

None.

#### Examples

```
MMHPP;
MMHPP:CMD=MNINI;
MMHPP:CLASS=PARAMETERS;
```

### Output Format

```
MMHPP;
Alarm
  ALLIP Alarm List Print
Reset
  RSBOI Restart Board Initiate
Status
  STSLP Status Signaling Link Print
  STPCP Status PCM Print
  STBOP Status Board Print
  STRLP Status Remote SIU Link Print
  STHLP Status Host Link Print
  STCGP Status Circuit Group Print
  STIPP Status IP Print
  STEPP Status of Ethernet Port Print
Etc.
  EXECUTED

mmhpp:cmd=cnsys;
CNSYS Configuration System Set
      This command is used to activate user parts, set the system
      network IP addresses and passwords.
      For this command to take effect a system restart is required.
Syntax : CNSYS: {[IPADDR=,][IPADDR2=,][SUBNET=,][SUBNET2=,]
         [GATEWAY=,][SCCP=,]
         [TCAP=,][MAP=,][PASSWORD=,][FTPPWD=]};
Example: CNSYS:IPADDR=123.124.125.126;
         CNSYS:MODE=SIUB;
         CNSYS:MAP=Y;
EXECUTED
```

## 6.12 Maintenance Commands

The maintenance commands include:

- MNINI - Maintenance Inhibit Initiate
- MNINE - Maintenance Inhibit End
- MNRSI - Maintenance Restart System Initiate

### 6.12.1 MNINI – Maintenance Inhibit Initiate

#### Synopsis

This command is used to deactivate an SS7 signaling link, SIGTRAN M3UA link, host RSI link or circuit group. The command is also used to inhibit an SS7 signaling link and to block a failed hard disk drive before removal and replacing.

***Important:*** In order to maintain RAID array hard disk drive integrity, you should follow the correct procedure detailed in Section 5.6.1, “SS7G31 and SS7G32 Hard Disk Drive RAID Management” on page 41.

***Note:*** To inhibit a signaling link, the command should be entered with the INHIBIT=Y parameter set. You should then use the STSLP MMI command to determine the (new) status of the link. If the inhibit request was accepted, the L3 STATE is shown as UNAVAILABLE. However, if the inhibit request was denied (for example, because it relates to the only active link), the L3 STATE is shown as AVAILABLE.

#### Syntax

```
MNINI: [SNLINK=,][INHIBIT=Y]] | [HOSTID=] | [GID=]; [LINK=,] [DRIVE=,]
```

#### Prerequisites

The following restrictions apply:

- If a link is to be inhibited, it must be active.
- The last link in a SS7 signaling link set can **not** be inhibited.
- The circuit group must be already configured and activated.
- The Disk drive must be active and not in the 'RESTARTING' state.

#### Attributes

Prompt - A *dangerous* command that must be confirmed by the operator.

#### Examples

```
MNINI:SNLINK=3;
MNINI:SNLINK=3,INHIBIT=Y;
MNINI:HOSTID=1;
MNINI:GID=4;
MNINI:LINK=4,INHIBIT=Y;
MNINI:DRIVE=0;
```

### 6.12.2 MNINE – Maintenance Inhibit End

#### Synopsis

This command is used to activate a previously inactive SS7 signaling link, SIGTRAN M3UA link, host RSI link or circuit group. The command is also used to uninhibit an SS7 signaling link and to unblock a newly installed hard disk drive following hard disk drive failure.

***Important:*** In order to maintain RAID array hard disk drive integrity, you should follow the correct procedure detailed in Section 5.6.1, “SS7G31 and SS7G32 Hard Disk Drive RAID Management” on page 41.

### Syntax

```
MNINE: [SNLINK=,[INHIBIT=]] | [HOSTID=] | [GID=]; [LINK=,] [DRIVE=,]
```

### Prerequisites

The following restrictions apply:

- When activating a link, the SS7 signaling link set has not already been activated.
- When uninhibiting a link, the link has been activated.
- The circuit group must be already configured and deactivated.
- The disk drive must be in the INACTIVE state.

### Attributes

None.

### Examples

```
MNINE:SNLINK=3;
MNINE:SNLINK=3,INHIBIT=N;
MNINE:HOSTID=1;
MNINE:GID=2;
MNINE:LINK=2,INHIBIT=N;
MNINE:DRIVE=0;
```

## 6.12.3 MNRSI – Maintenance Restart System Initiate

### Synopsis

This command restarts the entire system. All current log-on sessions are terminated. No change to the system configuration occurs and the state of all links is automatically restored when the system restart is complete. If SYSTYPE is set, the systems operating mode changes its system type after restart. Possible operating modes are:

- SWS - Signaling Web Services
- SGW – SIGTRAN Signaling Gateway
- SIU – Signaling Interface Unit
- TEST - The default mode of operation the server is shipped with and that does not require an operating mode specific license.

If software supporting a selected mode of operation has not been previously loaded (See page 2 of the CNSWP command) or is not in the process of being loaded (i.e., a new software binary has not been ftp'd into the siuftp account), then the system will automatically restart in its default operating mode

***Caution:*** If RESET is set to Y, then all diagnostic data in the “syslog” subdirectory of the siuftp account will be removed.

***Caution:*** If the RESTART parameter with a value of HALT is used, once the system has been halted, the only way to restart the unit is by physically pressing the Power switch on the front panel of the chassis.

### Syntax

```
MNRSI:[RESTART=,][SYSTYPE,][RESET=,];
```

### Prerequisites

The SYSTYPE parameter can only be set to system types that have been licensed for the unit.

### Attributes

None.

### Example

```
MNRSI;
MNRSI:RESTART=SOFT;
MNRSI:RESTART=SOFT,SYSTYPE=SGW;
MNRSI:RESTART=HALT;
```

## 6.13 Measurement Commands

The measurement commands include:

- MSEPP - Measurement Ethernet Port Print
- MSHLP - Measurement of Host Links Prints
- MSLCP - Measurement of License Capability Print
- MSMLP - Measurement Monitor link Print
- MSSYP - Measurement Remote Links Print
- MSPCP - Measurement PCM Print
- MSSLP - Measurement SS7 Link Print
- MSSTP - Measurement of SIGTRAN Links Print
- MSSYP - Measurement System Print
- MSSYP - Measurement Remote Links Print

### 6.13.1 MSEPP – Measurement Ethernet Port Print

#### Synopsis

This command prints the traffic measurements for each Ethernet port on the system taken over a period of time.

#### Syntax

```
MSEPP:[RESET=,][PAGE=];
```

#### Prerequisites

None.

#### Attributes

None.

#### Examples

```
MSEPP;
MSEPP:RESET=Y,PAGE=2;
```

#### Output Format

```
Ethernet Port Measurements (Page 1 of 2)
ETH RXKBYTE RXPKT  RXERR  RXDROP TXKBYTE TXPKT  TXERR TXDROP PERIOD
1   0       0      0      0      0       0      0     0      16:34:41
2   96324   135705 0      4204E5 28169   4444   0     0      16:34:41
3   0       0      0      0      0       0      0     0      16:34:41
4   3760    3273   0      33615  12503   3455   0     0      16:34:41
EXECUTED

Ethernet Port Measurements (Page 2 of 2)
ETH RXFIFO  RXFRAME RXCOMP RXMULT TXFIFO TXCOLLS TXCARRIER TXCOMP PERIOD
1   0       0       0      0      0      0       0          0     16:34:41
2   0       0       0      0      0      0       0          0     16:34:41
3   0       0       0      0      0      0       0          0     16:34:41
4   0       0       0      0      0      0       0          0     16:34:41
EXECUTED
```

The meaning of each field in the output is as follows:

- ETH (Dialogic® DSI SS7G31 Signaling Server). Ethernet port number in the range 1 to 4, where:
  - — ETH=1 corresponds to physical port 1
  - — ETH=2 corresponds to physical port 2
  - — ETH=3 corresponds to physical port 3
  - — ETH=4 corresponds to physical port 4

- ETH (Dialogic® DSI SS7G32 Signaling Server). Ethernet port number in the range 1 to 6, where:
  - ETH=1 corresponds to physical port 1
  - ETH=2 corresponds to physical port 2
  - ETH=3 corresponds to physical port ACT/LNK A (bottom)
  - ETH=4 corresponds to physical port ACT/LNK B (bottom)
  - ETH=5 corresponds to physical port ACT/LNK A (top)
  - ETH=6 corresponds to physical port ACT/LNK B (top)
- RXKBTYE - Number of kilobytes of data received (in kilobytes)
- RXPKT - Number of packets of data received
- RXERR - Number of receive errors detected
- RXDROP - Number of received packets dropped by the device driver during the measurement period
- TXKBTYE - Number of kilobytes of data transmitted (in kilobytes)
- TXPKT - Number of packets of data transmitted
- TXERR - Number of transmit errors detected
- TXDROP - Number of transmit packets
- PERIOD - The period over which the measurement was taken
- RXFIFO - The number of FIFO buffer errors received
- RXFRAME - The number of packet framing errors received
- RXCOMP - The number of compressed packets received
- RXMULT - The number of multicast frames received
- TXFIFO - The number of FIFO buffer error transmitted
- TXCOLLS - The number of collisions detected on the transmit side
- TXCARRIER - The number of carrier losses detected on the transmit side
- TXCOMP - The number of compressed packets transmitted

***Note:*** Values are reset using the RESET parameter. MSEPP:RESET=Y; resets the measurement values to 0.

### 6.13.2 MSHLP – Measurement of Host Links Prints

#### Synopsis

This command prints out traffic measurements for all configured SIU Host Links. Statistics are reset using the RESET parameter. MSHLP:RESET=Y resets the period and measurement values to 0.

#### Syntax

MSHLP: [RESET=];

#### Prerequisites

None.

#### Attributes

None.

#### Examples

MSHLP;

MSHLP:RESET=Y;

#### Output Format

MSHLP;

**Output Format**

```
Host Link Traffic Measurements
HOSTID RXMSG  TXMSG  RXOCT  TXOCT  OOSDUR NOOS   NDISCARD PERIOD
     1 1.43E6 1.45E6 5.48E6 5.35E6     62    1          0 00:14:55
     2 1.64E6 1.65E6 8.21E6 8.12E6     99    1          0 00:14:55
EXECUTED
```

The meaning of each field in the output is as follows:

- "RXMSG- Number of messages received over the link within the measurement period.
- "TXMSG - Number of messages transmitted over the link within the measurement period.
- "RXOCT - Number of octets received in messages over the link within the measurement period. Excludes the message header.
- "TXOCT - Number of octets transmitted in messages over the link within the measurement period. Excludes the message header.
- "OOSDUR - The total amount time the link was out of service during the measurement period (in multiples of 100ms).
- "NOOS - The number of times the link went out of service during the measurement period.
- "NDISCARD - The number of messages due to be transmitted on the link that were discarded during the measurement period.
- "PERIOD - The time period over which these statistics have been gathered (in hours, minutes and seconds).

### 6.13.3 MSLCP – Measurement of License Capability Print

**Synopsis**

This command prints the traffic measurements for each license on the system capable of supporting throughput licensing.

The meaning of each field in the output is as follows:

- **CAPABILITY** - A licensable capability of the system. This may be a protocol license or an operating mode license. A capability may have been purchased as a software license, shipped as part of the system or bundled as part of another license. If a capability is either not active on the system or doesn't provide measurements  then it will not be displayed.
- **RXDATA** - The amount of data received in Kilobytes during the measurement period.
- **TXDATA** - The amount of data transmitted in Kilobytes during the measurement period.
- **RXPEAK** - The peak received data rate in Kilobytes/s averaged over a rolling thirty second time window.
- **TXPEAK** - The peak transmit data rate in Kilobytes/s averaged over a rolling thirty second time window.
- **PEAK** - The peak data rate for both transmitted and received data in Kilobytes/s averaged over a rolling thirty second time window
- **CONGESTION** - The number of times the license has exceeded its throughput threshold.
- **ENFORCEMENT** - The number of times the unit has enforced the license throughput limit.
- **PERIOD** - Time since measurements on the route were last reset. Specified in hours, minutes and seconds.

***Note:*** Note: Values are reset using the RESET parameter. MSEPP:RESET=Y; resets the measurement values to 0.

**Syntax**

```
MSLCP:[RESET=,];
```

### Prerequisites

None.

### Attributes

None.

### Examples

```
MSLCP;
MSLCP:RESET=Y;
Output Format
Software License Capability Traffic Measurements
CAPABILITY RXDATA TXDATA RXPEAK TXPEAK PEAK CONG  ENFORCE PERIOD
M3UA       4204E5 3212E4 154    456     923 1     1       01:33:33
EXECUTED
```

## 6.13.4 MSMLP – Measurement Monitor link Print

### Synopsis

This command prints out traffic measurements for Monitor links.

Monitor link statistics are reset using the RESET parameter. MSMLP:RESET=Y resets the period and measurement values to 0.

### Syntax

```
MSMLP:[RESET=,][PAGE=];
```

### Prerequisites

None.

### Attributes

None.

### Examples

```
MSMLP;
MSMLP:RESET=Y,PAGE=2;
```

### Output Format

```
Monitor Link Measurements (Page 1 of 2)
LINK OOSDUR   RXOCT   RXMSU       PERIOD
0      0       3333    822         00:12:00
1      0       0       0           00:12:00
EXECUTED

Monitor Link Measurements (Page 2 of 2)
LINK FFRAME FRAME  MFRAME LFRAME ABORT  CRC    DISC   RBUSY  PERIOD
0     22      375    8220  16320 124306   0       0       3  00:12:00
1      0       0      333  4343  1233  434126     0       0  00:12:00
EXECUTED
```

The meaning of each field in the output is as follows:

- LINK - Monitor link
- OOSDUR - Duration that the link was not in service. This field is not currently supported.
- RXOCT - Number of Signaling Information Field (SIF) and Service Information Octet (SIO) octets received at Layer 2.
- RXMSU - Number of message signaling units octets received at Layer 2.
- FFRAME - The number of (error-free) frames received on the link, excluding any duplicate frames that are discarded as a result of the internal filtering mechanism.

- FRAME - The total number of (error-free) frames received on the link including any duplicate frames that are discarded as a result of the internal filtering mechanism.
- MFRAME - The number of misaligned frames (that is, frames that are not an integer multiple of 8 octets) received on the link.
- LFRAME - The number of received frames that were designated as either too long or too short for a configured protocol.
- ABORT - The number of aborts received on the link.
- CRC - Number of CRC errors received on the link.
- DISC - The number of times that the receiver was forced to discard incoming frames as a result of there being no internal buffers available to receive the incoming data. This is a count of the number of events rather than a count of the number of frames discarded.
- RBUSY - The number of times the receiver has entered the busy state as a result of the number of internal buffers falling below a set threshold.
- PERIOD - The period the measurement was taken over.

***Note:*** Values are reset using the RESET parameter. MSMLP:RESET=Y; resets the measurement values and period to 0.

### 6.13.5 MSRLP – Measurement Remote Links Print

#### Synopsis

This command prints out traffic measurements for all configured Remote SIU Links. Statistics are reset using the RESET parameter. MSRLP:RESET=Y resets the period and measurement values to 0.

#### Syntax

MSRLP: [RESET=];

#### Prerequisites

None.

#### Attributes

None.

#### Examples

MSRLP;

MSRLP:RESET=Y;

#### Output Format

MSRLP;

#### Output Format

```
Remote SIU Link Traffic Measurements
LINKID RXMSG  TXMSG  RXOCT  TXOCT  OOSDUR NOOS   NDISCARD PERIOD
     1 1.43E6 1.45E6 5.48E6 5.35E6     62    1          0 00:14:55
EXECUTED
```

The meaning of each field in the output is as follows:

- RXMSG- Number of messages received over the link within the measurement period.
- TXMSG - Number of messages transmitted over the link within the measurement period.
- RXOCT - Number of octets received in messages over the link within the measurement period. Excludes the message header.
- TXOCT - Number of octets transmitted in messages over the link within the measurement period. Excludes the message header.

- OOSDUR - The total amount time the link was out of service during the measurement period (in multiples of 100ms).
- NOOS - The number of times the link went out of service during the measurement period.
- NDISCARD - The number of messages due to be transmitted on the link that were discarded during the measurement period.
- PERIOD - The time period over which these statistics have been gathered (in hour, minutes and seconds).

### 6.13.6 MSPCP – Measurement PCM Print

#### Synopsis

This command prints out traffic measurements for PCMs. The measurements are cumulative between system startup and the next time the measurements are reset.

#### Syntax

```
MSPCP:[RESET=,];
```

#### Prerequisites

One or more PCMs must be configured using the LIU_CONFIG command in the config.txt file.

#### Attributes

None.

#### Examples

```
MSPCP;
MSPCP:RESET=Y;
```

#### Output Format

```
PCM Traffic Measurements
PORTID PCM    FMSLIP OUTSYN ERRSEC SEVSEC PERIOD
1      1-3    57     60     23     1      23:00:00
2      1-4    12     35     33     4      01:00:00
3      2-3    53     55     4      0      01:00:00
EXECUTED
```

The meaning of each field in the output is as follows:

- PORTID – Port ID as configured in config.txt file
- PCM – PCM on a board
- FMSLIP – Frame Slip count
- OUTSYN – Out-sync transitions
- ERRSEC – Errored Seconds count
- SEVSEC – Severely Errored Seconds count
- PERIOD – Time since measurements on the port were last reset. Specified in hours, minutes and seconds

***Note:*** PCM statistics are reset using the RESET parameter. MSPCP:RESET=Y; resets period and measurement values to 0.

### 6.13.7 MSSLP – Measurement SS7 Link Print

#### Synopsis

This command prints out traffic measurements for SS7 links.

SS7 link statistics are reset using the RESET parameter. MSSLP:RESET=Y resets the period and measurement values to 0.

#### Syntax

```
MSSLP:[RESET=,][PAGE=];
```

#### Prerequisites

None.

#### Attributes

None.

#### Examples

```
MSSLP;
MSSLP:RESET=Y,PAGE=2;
```

#### Output Format

```
SS7 link measurements (Page 1 of 2)
LINK OOSDUR RXNACK RXMSU RXOCT TXMSU TXOCT   RTXOCT NCONG PERIOD
0    0      0      375   8220  16320 124306  0      0     00:12:00
1    0      0      392   8624  17036 141860  0      0     00:12:00
EXECUTED

SS7 link measurements (page 2 of 2)
LINK ALIGN   SUERR   TBUSY   TCONG   NDISCARD NEVENT  PERIOD
0    0       0       0       0       0        0        00:12:00
1    0       0       0       0       0        0        00:12:00
EXECUTED
```

The meaning of each field in the output is as follows:

- LINK – SS7 signaling link
- OOSDUR – Duration that the link was not in service. This field is **not** currently supported.
- RXNACK – Number of negative acknowledgements received. Not applicable for SS7 links that are IP-based.
- RXMSU – Number of message signaling units octets received
- RXOCT – Number of Signaling Information Field (SIF) and Service Information Octet (SIO) octets received
- TXMSU – Number of message signaling units octets transmitted
- TXOCT – Number of SIF and SIO octets transmitted
- RTXOCT – Octets retransmitted
- NCONG – Congestion counter
- PERIOD –This field is not currently supported
- ALIGN - Number of failed signaling link alignment attempts
- SUERR - Number of signal units in error
- TBUSY - Duration of local busy condition
- CONG - Duration of link congestion
- NDISCARD - Number of MSUs discarded due to congestion
- NEVENT - Number of congestion events leading to MSU discard

***Note:*** Values are reset using the RESET parameter. MSSLP:RESET=Y; resets the measurement values to 0.

### 6.13.8 MSSTP – Measurement of SIGTRAN Links Print

#### Synopsis

This command prints out traffic measurements for SIGTRAN links. Link statistics are reset using the RESET parameter. MSSTP:RESET=Y resets the period and measurement values to 0. If TYPE is specified only configured links of the type are displayed.

#### Syntax

MSSTP:[SNLINK=,][TYPE=,][RESET=];

#### Prerequisites

None.

#### Attributes

None.

#### Examples

```
MSSTP;
MSSTP:RESET=Y;
MSSTP:TYPE=M3UA ;
```

#### Output Format

```
<msstp;
SIGTRAN Link Traffic Measurements
SNLINK TYPE  RXCK    TXCK    RTXCK  NOOS    OSDUR  PERIOD
1      M3UA  1.43E6 1.45E6 115    1       62     00:14:55
2      M2PA  1.64E6 1.65E6 99     1       98     00:14:55
EXECUTED
```

The meaning of each field in the output is as follows:

- SNLINK - SIGTRAN signaling link.
- RXCK - Chunks of SCTP data received.
- TXCK - Chunks of SCTP data transmitted.
- RTXCK - Chunks of SCTP data re-transmitted.
- NOOS - Number of times a SIGTRAN link has been aborted or shutdown.
- OOSDUR - Duration (seconds) that the link was not in service.
- PERIOD - Elapsed time since measurements were reset.

### 6.13.9 MSSYP – Measurement System Print

#### Synopsis

This command prints out system related measurements for load and congestion taken over a period of time.

#### Syntax

MSSYP:[RESET=,];

#### Prerequisites

None.

#### Attributes

None.

#### Example

```
MSSYP;
```

### Output Format

```
System Measurements
NOVLD      0
MAXLOAD    28.81%
LOADAVG    2.28%
PERIOD     18:36:55
EXECUTED
```

The meaning of each field in the output is as follows:

- NOVLD - The number of periods of congestion (overload) during the measurement period.
- MAXLOAD - Maximum load average measurement taken over 1 minute (based on the UNIX load average)
- LOADAVG - The average load on the system (based on the UNIX load average) measurement taken over the measurement period.
- PERIOD - The period the measurement was taken over.

***Note:*** Values are reset using the RESET parameter. MSSYP:RESET=Y; resets the measurement values to 0.

## 6.14 Reset Command

The reset command is:

- RSBOI - Reset Board Initiate

### 6.14.1 RSBOI – Reset Board Initiate

#### Synopsis

This command resets a board. The board is reconfigured from the system configuration data.

***Note:*** All PCMs are taken out of service temporarily while the reset occurs. All SS7 links that use either timeslots or SP channels on the board are also taken out of service temporarily. If the board is acting as the clock source for the system, then the board with the next highest clock priority becomes the clock master while the reset occurs.

#### Syntax

```
RSBOI:BPOS=;
```

#### Prerequisites

The board must have already been initialized.

#### Attributes

Prompt - A *dangerous* command that must be confirmed by the operator.

#### Example

```
RSBOI:BPOS=1;
```

## 6.15 Status Commands

The status commands include:

- STALP - Status Alarm Print
- STBOP - Status Board Print
- STCGP - Status Circuit Group Print
- STCRP - Status SS7 Route Print
- STDDP - Status Disk Drive Print
- STEPP - Status Ethernet Port Print
- STHLP - Status Host Link Print
- STIPP - Status IP Print
- STLCP - Status Licensing Print
- STMLP - Status Monitor Link Print
- STPCP - Status PCM Print
- STRAP - Status Remote Application Server Print
- STRLP - Status Remote SIU Link Print
- STSLP - Status SS7 Link Print
- STSRP - Status SIGTRAN Route Print
- STSSP - Status Sub-System Resource Print
- STSTP - SIGTRAN Link Status
- STSYP - Status System Print
- STTDP - Status TCAP Dialog Print
- STTPP - Network Time Protocol Status Print
- STTRP - Status TCAP Resource Print

### 6.15.1 STALP – Status Alarm Print

#### Synopsis

This command displays counts for current alarms within the system.

#### Syntax

```
STALP;
```

#### Prerequisites

None.

#### Attributes

None.

#### Example

```
STALP;
```

#### Output Format

```
Alarm Status

SYS PCM SIG MNR  MAJ  CRT
1   0   1    2    0    0
EXECUTED
```

The meaning of each field in the output is as follows:

- SYS – The number of system alarms.
- PCM – The number of PCM alarms.
- SIG – The number of signaling alarms.
- MNR – The number of minor alarms.
- MAJ – The number of major alarms.
- CRT – The number of critical alarms.

### 6.15.2 STBOP – Status Board Print

#### Synopsis

This command requests a printout of the status of all configured signaling boards. Possible status values are:

- INACTIVE - The board is not in operation.
- RESETTING - The board is undergoing a reset.
- ACTIVE - The board is operational.
- FAILED - The board has failed and is out of service.

#### Syntax

```
STBOP;
```

#### Prerequisites

None.

#### Attributes

None.

#### Example

```
STBOP;
```

#### Output Format

```
Board status
BPOS    BTYPE  STATE
1       SS7HDP ACTIVE
3       SS7HDP ACTIVE
EXECUTED
```

### 6.15.3 STCGP – Status Circuit Group Print

#### Synopsis

This command requests a printout of the status of the configured circuit groups. If GID (circuit group identifier) is specified, the status for that specific circuit group is displayed. If no GID is specified, then the status of all circuit groups is displayed.

#### Syntax

```
STCGP[:GID=];
```

#### Prerequisites

None.

#### Attributes

None.

### Examples

```
STCGP;
STCGP:GID=2;
```

### Output Format

```
Circuit Group Status
GID  TYPE     CICS   MAINT  ACTIVE IDLE
0    INACTIVE
1    S        15     3      5      7
2    D        15     3      5      7
EXECUTED
```

The meaning of each field in the output is as follows:

- TYPE – Indicates whether the command was configured dynamically (D) using IPC messages or statically (S) using the config.txt file. If the group was configured statically, and not activated, an INACTIVE indication is shown and all other parameters on the row are shown as blank.
- CICS – The number of Circuit Identification Codes (CICs) assigned to the circuit group.
- MAINT – The number of circuits that do not have calls in progress and have an active maintenance state (and therefore are not available for selection).
- ACTIVE – The number of circuits that have calls in progress.
- IDLE – The number of circuits that do not have calls in progress, but are available for selection.

## 6.15.4 STCRP – Status SS7 Route Print

### Synopsis

This command shows the status of all configured SS7 routes.

### Syntax

```
STCRP;
```

### Prerequisites

None.

### Attributes

None.

### Example

```
STCRP;
```

### Output Format

```
CCS SS7 route status
ROUTE NC DPC       ROUTE STATUS CONG LEVEL LS1 STATUS     LS2 STATUS
1     1  1021      Available    0          Available
2     1  2171      Available    0          Available      Available
3     2  51        Unavailable  0          Unavailable
EXECUTED
```

The meaning of each field in the output is as follows:

- ROUTE - Logical reference for an SS7 route
- NC - SS7 Network Context
- ROUTE STATUS - Possible values are:
  - — Available - The route is available for traffic to the remote point code of the route.
  - — Unavailable - The route is unavailable for traffic to the remote point code of the route.
- CONG LEVEL - Possible values are:
  - — 0, no congestion
  - — 1, 2, or 3 indicates the ITU/ANSI congestion level

- LS1 STATUS and LS2 STATUS - Possible values are:
  - — Available - The link set on the route is available for traffic to the adjacent point code.
  - — Unavailable - The link set on the route is unavailable for traffic to the adjacent point code.

### 6.15.5 STDDP – Status Disk Drive Print

#### Synopsis

This command displays the status of hard disk drives within the RAID array.

#### Syntax

```
STDDP;
```

#### Prerequisites

None.

#### Attributes

None.

#### Example

```
STDDP;
```

#### Output Format

```
STDDP;
Disk Drive Status
DRIVE STATUS
0     UP
1     UP
EXECUTED
```

The STATUS field will display one of the following values:

- UP – The disk drive is operational. If the disk forms part of a RAID array then all the RAID devices on this drive are in an “active sync state”.
- DOWN– The disk drive is non operational. If the disk forms part of a RAID array then one or more of the Raid devices on this drive is faulty.
- RESTARTING – One or more of the raid devices on this drive is synchronizing with another Raid device. The disk is considered “non operational” until synchronization is complete.
- INACTIVE – The drive is not configured as part of the RAID array and therefore is not in use. This may be due to user action through MMI, the drive not being physically present at startup or a failed drive being removed by the operating software at startup from the RAID array.

***Caution:*** Before replacing a failed drive, the drive must first be taken out of service using the MNINI command. Once the replacement drive is in place, the disk can be restored to service using the MNINE command. See Section 5.6.1, “SS7G31 and SS7G32 Hard Disk Drive RAID Management” on page 41.

### 6.15.6 STEPP – Status Ethernet Port Print

#### Synopsis

This command provides the status of Ethernet ports on the system.

#### Syntax

```
STEPP;
```

#### Prerequisites

None.

### Attributes

None.

### Example

```
STEPP;
```

### Output Format

```
ETH PARTNER SPEED DUPLEX STATUS
1                    DOWN
2           100   FULL   UP
3   4       1000  FULL   ACTIVE
4   3       1000  FULL   STANDBY
EXECUTED
```

The meaning of each field in the output is as follows:

- ETH – The Ethernet port identity.
- PARTNER – Identifies the other port member of a port bonding team.
- SPEED – The speed of the Ethernet port in MHz (10, 100 or 1000).
- DUPLEX – Whether the port is FULL or HALF duplex.
- STATUS – Whether the port is UP or DOWN. If the port is in a team, and it is “up”, the status indicates instead whether the port is ACTIVE or in STANDBY.

## 6.15.7 STHLP – Status Host Link Print

### Synopsis

This command requests a printout of the status of all configured SIU-Host Links.

### Syntax

```
STHLP;
```

### Prerequisites

None.

### Attributes

None.

### Example

```
STHLP;
```

### Output Format

```
Host link status
HOSTID      RSI STATE    FOREIGN IPADDR          TCP STATE
0          *FAILED       0.0.0.0                 LISTEN
1           ACTIVE       123.124.125.126         ESTABLISHED
EXECUTED
```

Possible STATE values are:

- ACTIVE
- FAILED
- DEACTIVATED

***Note:*** The asterisk (*) indicates that the host is acting as a management host.

Possible TCP STATE values are:

- CLOSED
- LISTEN

- SYNC SENT
- SYNC RECEIVED
- ESTABLISHED
- CLOSE WAIT
- FIN WAIT 1
- CLOSING
- LAST ACK
- FIN WAIT 2
- TIME WAIT
- UNKNOWN, if this information is not available.

### 6.15.8 STIPP – Status IP Print

#### Synopsis

This command sends four ICPM (Internet Control and Management Protocol) Echo Request frames to the specified remote IP address and measures the maximum round trip time, similar to the standard UNIX ping command.

#### Syntax

```
STIPP:IPADDR=;
```

#### Prerequisites

None.

#### Attributes

None.

#### Example

```
STIPP:IPADDR=123.124.125.126;
```

#### Output Format

```
IPADDR                  SEND      RECV      MAXRTD
123.125.125.126         4         4         20
EXECUTED
```

The meaning of each field in the output is as follows:

- IPADDR – The IP address to which the five ICPM Echo Request frames are to be sent.
- SEND – Shows the number of frames transmitted.
- RECV – Shows the number of replies received
- MAXRTD – Shows the maximum delay between sending a frame and receiving a reply, in milliseconds. The measurement is accurate to 10ms, hence any value less than 10ms is displayed as “<10”.

***Note:*** If the destination IP address is not reachable, RECV is shown as 0 and MAXRTD is shown as “-”.

### 6.15.9 STLCP – Status Licensing Print

This command prints the status of each license on the system.

The meaning of each field in the output is as follows:

- CAPABILITY — A licensable capability of the system. This may be a protocol license or an operating mode license. A capability may have been purchased as a software license, shipped as part of the system or bundled as part of another license.
- STATUS — Status of the capability on the system where:
  - NONE — This capability is not present. It requires a software license.
  - INACTIVE — The license is present but not running for software reasons, e.g., the license is for a different mode of operation or the capability is dependant on another capability that is not active.
  - DEACTIVATED — The license is present but not running due to configuration reasons (it has been user deactivated in CNSYS).
  - ACTIVE — The license is active.
  - ERROR — This capability cannot be activated as it depends on a software license which his not present (e.g., TCAP is present but SCCP is not).
  - RESTART — The license is present but requires a system restart to allow activation.
  - CONGESTED — The throughput congestion level has been reached for the capability.
  - ENFORCED — The licensed traffic rate has been exceeded for a extended period and the system is now limiting traffic to the licensed rate for the capability.
- LINKS — The licensed number of links for the capability. Blank means not applicable.
- RATE — The licensed throughput rate in Kilobytes/s for the capability. Blank means not applicable.
- CREDIT — The current throughput account credit if applicable. The throughput account credit is expressed as a % of the maximum account credit.

***Note:*** The maximum account credit is the licensed throughput rate * 30. The throughput account credit is decremented each time traffic passes through the system. The throughput account is incremented every second by the value of the licensed throughput rate. If the licensed throughput is exceeded for a sustained period of time the credit available will drop. When the credit drops to 50% of the maximum throughput credit a congestion alarm will fire. When the credit drops to 0% (i.e., there is no credit left) throughput enforcement will occur limiting throughput to the licensed rate. Throughput enforcement will be maintained until the account credit returns to 75% or above of the maximum throughput credit.

#### Syntax

```
STLCP;
```

#### Prerequisites

None.

#### Attributes

None.

#### Examples

```
STLCP;
```

### Output Format

```
stlcp;
Software License Capability Status
CAPABILITY   STATUS       LINKS   SESSIONS RATE    CREDIT
SIU          ACTIVE
SGW          INACTIVE
DSC          NONE
SCTP         ACTIVE
M2PA         ACTIVE       256              2460    100
M3UA         ACTIVE       256              2460    100
MTP          ACTIVE       192
SCCPCL       ACTIVE
SCCPCO       ACTIVE
TCAP         ACTIVE
MAP          ACTIVE
SNMP         ACTIVE
EXECUTED
```

### 6.15.10 STMLP – Status Monitor Link Print

#### Synopsis

This command requests a printout of the status of configured Monitor links. If the LINK parameter is specified, the status of the corresponding link is displayed. If the LINK parameter is not specified, the status of all configured Monitor links is displayed.

The command will use the presence (or absence) of LSSU signaling units to determine whether the monitored-link link state is IN-SERVICE or OUT-OF-SERVICE

#### Syntax

```
STMLP:[LINK=,];
```

#### Prerequisites

None.

#### Attributes

None.

#### Examples

```
STMLP;
STMLP:LINK=1;
```

#### Output Format

```
Monitor link status
LINK L2 STATE
0    OUT OF SERVICE
1    IN SERVICE
2    IN SERVICE
3    IN SERVICE
4    IN SERVICE
5    IN SERVICE
EXECUTED
```

The meaning of each field in the output is as follows:

- LINK - Shows the value of the link_id parameter for that link as configured using the MONITOR_LINK command in the config.txt file.
- L2 STATUS - L2 status; possible values are:
  - IN SERVICE
  - OUT OF SERVICE

### 6.15.11 STPCP – Status PCM Print

#### Synopsis

This command requests a printout of the status of all configured PCM ports.

#### Syntax

```
STPCP;
```

#### Prerequisites

None.

#### Attributes

None.

### Example

```
STPCP;
```

### Output Format

```
PCM status
PORTID PCM  SYNCPRI PCM STATUS    CLOCK STATUS
0      1-3  *       OK            STAND ALONE
2      2-1  1       OK            ACTIVE
3      2-2  31      OK            OK
5      2-4  0       BER > 1:10^5  FAULT
EXECUTED
```

Possible PCM STATUS values are:

- PCM LOSS - No signal sensed on the PCM input.
- AIS - The remote side sends all ones indicating that there is an error condition, or it is not initialized.
- SYNC LOSS - Loss of frame alignment since no frame synchronization has been received
- REMOTE ALARM - The remote end indicates that is it is OK, but also indicates that it is detecting an error condition.
- BER > 1:10^3 - The PCM is encountering a Bit Error Rate (BER) of 10^3.
- BER > 1:10^5 - The PCM is encountering a BER of 10^5.
- OK - The PCM is operational.

Possible CLOCK STATUS values are:

- FAULT - The PCM is unable to provide clock for the SIU due to a fault on the board.
- NOT OK - The PCM is not a valid clock source.
- ACTIVE - The PCM is a valid clock source and is currently providing clock for the SIU.
- OK - The PCM is a valid clock source but is currently **not** providing clock for the SIU.
- STANDBY - The PCM is a valid clock source and will provide clock for the SIU in the event of failure of the ACTIVE clock source.
- STAND ALONE - Telephony bus disabled.

***Note:*** When the internal telephony bus is disabled in the board, the asterisk symbol (*) is displayed in the SYNCPRI field and the CLOCK STATUS is set to STAND ALONE.

## 6.15.12 STRAP – Status Remote Application Server Print

This command provides the status of SIGTRAN Remote Application Servers. It also provides the status of a link associated with the server.

Definitions of the AS status:

- AVAILABLE - The AS is available.
- UNAVAILABLE - The AS is unavailable.
- INSUFF_ASP - The AS is available but it has insufficient ASPs active as configured by the STN_RAS command (only valid for load sharing).

Definitions of the ASP within the server:

- DOWN - The link attached to the server is down.
- ACTIVE - The link attached to the server is active.
- INACTIVE - The link attached to the server is inactive.

Definitions of TRMD (Traffic Mode):

- LS - Load sharing mode.
- OR - Override mode.
- BC - Broadcast mode.

#### Syntax

```
STRAP:[RAS=];
```

#### Prerequisites

The specified Remote Application Server must be configured and active.

#### Attributes

None.

#### Example

```
STRAP;
```

#### Output Format

```
Status Remote Application Server Print
RAS  NC   DPC       RC      SNLINK  AS STATUS     ASP STATUS  TRMD
1     0   55        1       1       AVAILABLE     AVAILABLE   LS
1     0   55        1       2       AVAILABLE     DOWN        LS
EXECUTED
```

### 6.15.13 STRLP – Status Remote SIU Link Print

#### Synopsis

This command requests a printout of the status of the configured inter-SIU Ethernet link.

#### Syntax

```
STRLP;
```

#### Prerequisites

None.

#### Attributes

None.

#### Example

```
STRLP;
```

#### Output Format

```
Remote link status
LINKID      RSI STATE    FOREIGN IPADDR          TCP STATE
0           ACTIVE       123.124.125.126         ESTABLISHED
```

Possible RSI STATE values are:

- ACTIVE
- FAILED

Possible TCP STATE values are:

- CLOSED
- LISTEN
- SYNC SENT
- SYNC RECEIVED
- ESTABLISHED
- CLOSE WAIT
- FIN WAIT 1
- CLOSING

- LAST ACK
- FIN WAIT 2
- TIME WAIT
- UNKNOWN if this information is not available

### 6.15.14 STSLP – Status SS7 Link Print

#### Synopsis

This command requests a printout of the status of configured SS7 signaling links. If the LINK parameter is specified, the status of the corresponding link is displayed. If the LINK parameter is not specified, the status of all configured SS7 signaling links is displayed.

#### Syntax

```
STSLP:[LINK=,];
```

#### Prerequisites

None.

#### Attributes

None.

#### Examples

```
STSLP;
STSLP:LINK=1;
```

#### Output Format

```
SS7 link status
LINK   L2 STATE       L3 STATE     L3 BLOCKING STATUS
0      OUT OF SERVICE UNAVAILABLE  ---- ---- ---- ---- ---- ---- ----
1      IN SERVICE     AVAILABLE  INHL INHR ---- ---- ---- ---- ----
2      IN SERVICE     AVAILABLE  INHL ---- ---- ---- ---- ---- ----
3      IN SERVICE     AVAILABLE  INHL ---- ---- ---- ---- ---- ----
4      IN SERVICE     AVAILABLE    ---- ---- ---- ---- CBIP ---- ----
5      IN SERVICE     AVAILABLE    ---- ---- ---- ---- ---- LIIP ----
EXECUTED
```

The meaning of each field in the output is as follows:

- LINK - Shows the value of the **link_id** parameter for that link as configured using the MTP_LINK command in the config.txt file.
- L2 STATUS - L2 status; possible values are:
  - IN SERVICE
  - OUT OF SERVICE
  - PROCESSOR OUTAGE
  - ALIGNED READY
  - INITIAL ALIGNMENT
  - ALIGNED NOT RDY
- L3 STATUS - L3 status, possible values are:
  - AVAILABLE
  - UNAVAILABLE
  - CONGESTED
  - DEACTIVATED (the link has been deactivated by the user)
- L3 BLOCKING STATUS - Possible values are:
  - INHR - The Link is remotely inhibited
  - INHL - The Link is locally inhibited

— BLKR - The Link is remotely blocked
— COIP - Changeover is in progress
— CBIP - Changeback is in progress
— LIIP - Local link inhibiting is in progress
— LUIP- Local link uninhibiting is in progress

### 6.15.15 STSRP – Status SIGTRAN Route Print

This command requests a status of a SIGTRAN Route.

Status of a SIGTRAN Route:

- BLOCKED - The Gateway route is blocked.
- AVAILABLE - The Point Code is available over this route.
- UNAVAILABLE - The Point Code is unavailable over this route.

Status of a Gateway associated with the route:

- AVAILABLE - The gateway is available.
- UNAVAILABLE - The gateway is unavailable.

#### Syntax

```
STSRP=[SNRT=];
```

#### Prerequisites

If specified the SIGTRAN Route must be configured.

#### Attributes

None.

#### Example

```
STSRP;
```

#### Output Format

```
SIGTRAN Route Status
SNRT  NC  DPC       SG RT STATUS        GW STATUS
1     1   664       1  AVAILABLE        UNAVAILABLE
1     1   664       2  AVAILABLE        AVAILABLE
2     1   56444     2  AVAILABLE        AVAILABLE
3     1   3334      1  UNAVAILABLE      UNAVAILABLE
EXECUTED

****************
```

### 6.15.16 STSSP – Status Sub-System Resource Print

#### Synopsis

This command requests a printout of the status of Sub-System Resources. If the ID parameter is specified, the status of the corresponding SSR identified by the ID is displayed. If the ID parameter is not specified, the status of all configured SSRs is displayed.

#### Syntax

```
STSSP:[ID=,];
```

#### Prerequisites

None.

#### Attributes

None.

#### Examples

```
STSSP;
STSSP:ID=1;
```

#### Output Format

```
Sub-System Resource Status
ID  NC  Type  SSN   SPC   State
3   0   RSS   12    3226  ALLOWED
4   1   RSP         3229  PROHIBITED
5   0   LSS   12          ALLOWED
EXECUTED
```

Possible values of “State” are:

- PROHIBITED - Sub-system resource Prohibited
- ALLOWED - Sub-system resource Allowed

### 6.15.17 STSTP – SIGTRAN Link Status

#### Synopsis

This command requests a printout of the status of configured SIGTRAN signaling links. If the LINK parameter is specified, the status of the corresponding link is displayed. If the LINK parameter is not specified, the status of all configured SIGTRAN signaling links are displayed. If TYPE is specified only configured links of the type are displayed.

#### Syntax

```
STSTP:[SNLINK=,][TYPE=,][PAGE=,];
```

#### Prerequisites

If specified, the SNLINK should already be configured.

#### Attributes

None.

#### Examples

```
STSTP;
STSTP:SNLINK=1;
STSTP:TYPE=M3UA,PAGE=2;
```

### Output format

```
<ststp;
SIGTRAN Signaling Link Status (Page 1 of 2)
SNLINK  TYPE  SP STATUS    SCTP STATUS
1       M3UA  AVAILABLE    ESTABLISHED
2       M2PA               ESTABLISHED
EXECUTED

<ststp:page=2;
SIGTRAN Signaling Link Status (Page 2 of 2)
SNLINK  TYPE IPADDR STATUS IPADDR RTO IPADDR2 STATUS IPADDR2 RTO
1       M3UA ACTIVE        500        Not Configured
2       M2PA ACTIVE        500        Not Configured
EXECUTED
```

***Note:*** M2PA links do not display SP STATUS.

The retransmission timeout (RTO) is a time between 500 and 6000 milliseconds when SCTP waits before retransmitting an octet. The RTO value dynamically changes according to line conditions and provides an indication of the quality of the connection to the remote IP address.

SCTP STATUS can be one of the following values:

- FAILED - The association is being configured.
- CLOSED - Association is closed.
- COOKIE WAIT - Association is waiting for a cookie.
- COOKIE ECHOED - Association has echoed a cookie.
- ESTABLISHED - Association is established.
- PENDING SHUTDOWN - Association is pending shutdown.
- SENT SHUTDOWN- Association has sent shutdown.
- RCVD SHUTDOWN - Association has received shutdown.
- SHUTDOWN. - Association has shutdown.

## 6.15.18 STSYP – Status System Print

### Synopsis

This command provides a summary of the load, uptime and alarms on the system.

### Syntax

```
STSYP;
```

### Prerequisites

None.

### Attributes

None.

### Examples

```
STSYP;
```

### Output Format

```
System Status
CPU:       2 X Intel(R) Xeon(TM) CPU 2.4GHz
MEMORY     1024MB
UPTIME     09:04:02
NRESTART   5
LOADAVG1   28.81%
LOADAVG5   2.28%
LOADAVG15  1.35%
ALMSYS     1
ALMPCM     0
ALMSIG     1
MINOR      2
MAJOR      0
CRITICAL   0
EXECUTED
```

The meaning of each field in the output is as follows:

- CPU - A string identifying the CPU type and speed
- MEMORY - The amount of RAM in the system
- UPTIME - The length of time the application software has been running
- NRESTART - The number of times the system has restarted since factory installation
- LOADAVG1 - The UNIX load average measurement taken over 1 minute
- LOADAVG5 - The UNIX load average measurement taken over 5 minutes
- LOADAVG15 - The UNIX load average measurement taken over 15 minutes
- ALMSYS - The number of system alarms
- ALMPCM - The number of PCM alarms
- SIG - The number of signaling alarms
- MINOR - The number of minor alarms
- MAJOR - The number of major alarms
- CRITICAL - The number of critical alarms

## 6.15.19 STTDP – Status TCAP Dialog Print

### Synopsis

This command allows you to read the status of a single TCAP dialog or a range of dialogs. If a RANGE value is specified, the status of each dialog in the range starting from the dialog identified by DLGID is displayed. The default value of DLGID is 0. If a RANGE value is not specified, the range is assumed to be one, therefore only the status of the single dialog identified by DLGID is displayed.

### Syntax

```
STTDP:[DLGID=],[RANGE=];
```

### Prerequisites

TCAP must be licensed and enabled.

### Attributes

None.

### Example

```
STTDP:DLGID=122,RANGE=2;
```

### Output Format

```
STTDP;
TCAP dialogue status
DLG     DHA      TSM      DCS       INVK     LTRID      RTRID
122     IDLE     IDLE     FREE      0
123     ACTIVE   ACTIVE   ACTIVE    5        0000C040   0000C080
EXECUTED
```

The meaning of each field in the output is as follows:

- DHA – TCAP dialog handler state. Possible values are: IDLE, RCVD, SENT, ACTIVE
- TSM – TCAP dialog transaction state. Possible values are: IDLE, RCVD, SENT, ACTIVE
- DCS – TCAP dialog control structure state. Possible values are: FREE, PENDING, ACTIVE, ISM
- INVK – Number of active invokes in the dialog
- LTRID – Local transaction ID
- RTRID – Remote transaction ID

## 6.15.20 STTPP – Network Time Protocol Status Print

### Synopsis

This command is used to display the status of the Network Time Protocol servers configured on the unit.

### Syntax

```
STTPP;
```

### Prerequisites

None.

### Attributes

None.

### Example

```
STTPP;
Status of NTP Servers
NTPSER IPADDR          STATUS      STRATUM OFFSET    LABEL
1      192.168.0.1     SYSPEER     3       -0.025594 NTPSERV1
2      192.168.0.2     ACTIVE      4       -0.025477 NTPSERV2
EXECUTED
```

### Description

Meaning of fields in the print command:

- **Status**

| Status | Description |
|---|---|
| INACTIVE | The NTP service is disabled. |
| UNREACHABLE | The NTP server is unreachable. |
| REJECT | The NTP server has been rejected by the server selection algorithm. |
| ACTIVE | NTP time information is being received from this server. |
| SYSPEER | NTP has selected this server to synchronize to. |

- **Stratum**
  The NTP Stratum value reported by the NTP server.

- **Offset**
  The difference in seconds between the clock (UTC) as configured on the unit and the UTC time as reported by the NTP server. The offset must be within 1000 seconds of the current system time for synchronisation with this NTP server to occur.

### 6.15.21 STTRP – Status TCAP Resource Print

#### Synopsis

This command shows a summary of the status of TCAP resources on the unit. The command STTDP can be used to get details of a specific dialog or range of dialogs.

#### Syntax

```
STTRP;
```

#### Prerequisites

None.

#### Attributes

None.

#### Example

```
STTRP;
```

#### Output Format

```
TCAP resource status
ICD    OGD    INVK   CPT    DBUF
122    12233  2222   222    22
EXECUTED
```

The meaning of each field in the output is as follows:

- ICD – Number of active incoming dialogs. These are dialogs that have been initiated by a remote system.
- OGD – Number of active outgoing dialogs. These are dialogs that have been initiated by the local host.
- INVK – Number of active invokes. These Invoke structures are only required for locally initiated Invokes and are not used for received Invoke operations.
- CPT – Number of allocated component structures. These are used temporarily for pending component requests until an appropriate dialog request is received.
- DBUF – Number of allocated dialog buffers. These are used temporarily for building dialog request messages from pending components.

## 6.16 Network Time Protocol

The Network Time Protocol, NTP, allows synchronization of the internal system clock with an external time source thus providing greater accuracy for system alarm events and SNMP trap notifications.

NTP can be activated using the CNTDS (set time and date) command, while up to 16 remote NTP servers can be configured using the CNTPI command. The current status of the NTP servers can be identified using the STTPP command.

The current system time must be within 1000 seconds (just over 15 minutes) of the time currently used by an active NTP server for NTP time synchronization to be successful. If the time is not within that range, then NTP synchronization will fail, the STTPP command will indicate that the NTP servers are INACTIVE and the system will continue to use its current time. In this event, if the user wishes to use time based on that used by the NTP servers, then the user should modify system time using CNTDS to be within 1000 seconds, after which the signaling server will automatically re-attempt synchronization.

## 6.17 Command Summary

The following is a summary of the command categories and the commands within those categories:

**Alarms Commands**

- ALLIP - Alarm List Print

**Configuration Commands**

- CNBUI - Configuration Backup Initiate
- CNBUS - Configuration Backup Set
- CNCRP - Configuration MTP Route Print
- CNCSP - Configuration Concerned Subsystem Print
- CNGAP - Configuration GTT Address Print
- CNGLP - Configuration SIGTRAN Gateway List
- CNGPP - Configuration GTT Pattern Print
- CNGTP - Configuration Global Title Translation Print
- CNGLP - Configuration SIGTRAN Gateway List
- CNOBP - Display TRAP Configuration
- CNOBS - Set TRAP Configuration
- CNRDI - Configuration Restore Defaults Initiate
- CNSMC - Change SNMP Manager Configuration
- CNSME - End SNMP Manager Configuration
- CNSMI - Set SNMP Manager Configuration
- CNSMP - Display SNMP Manager Configuration
- CNSNP - Configuration SNMP Print
- CNSNS - Configuration SNMP Set
- CNSRP - Configuration SIGTRAN Route Print
- CNSSP - Configuration Subsystem Resource Print
- CNSWP - Configuration Software Print
- CNSYP - Configuration System Print
- CNSYS - Configuration System Set
- CNTDP - Configuration Time and Date Print
- CNTDS - Configuration Time and Date Set
- CNTMP - Configuration Trace Mask Print
- CNTMS - Configuration Trace Mask Set
- CNTPE - Configuration Network Time Protocol Server End
- CNTPI - Configuration Network Time Protocol Server Initiate
- CNTPP - Configuration Network Time Protocol Print
- CNUPI - Configuration Update Initiate
- CNURC - Configuration Update Resource Change
- CNURE - Configuration Update Resource End
- CNURI - Configuration Update Resource Initiate
- CNUSC - Change SNMP v3 User Configuration
- CNUSE - End SNMP v3
- CNUSI - Set SNMP v3
- CNUSP - Display SNMP v3

**IP Commands**

- IPEPS - Set Ethernet Port Configuration
- IPEPP - Display Ethernet Port Configuration
- IPGWI - Internet Protocol Gateway Initiate
- IPGWE - Internet Protocol Gateway End
- IPGWP - Internet Protocol Gateway Print

**MML Commands**

- MMLOI - MML Log Off Initiate
- MMHPP - MML Help Print

Maintenance Commands

- MNINI - Maintenance Inhibit Initiate
- MNINE - Maintenance Inhibit End
- MNRSI - Maintenance Restart System Initiate

**Measurement Commands**

- MSEPP - Measurement Ethernet Port Print
- MSLCP - Measurement of License Capability Print
- MSPCP - Measurement PCM Print
- MSSLP - Measurement SS7 Link Print
- MSSTP - Measurement of SIGTRAN Links Print
- MSSYP - Measurement System Print

**Reset Command**

- RSBOI - Reset Board Initiate

**Status Commands**

- STALP - Status Alarm Print
- STBOP - Status Board Print
- STCGP - Status Circuit Group Print
- STCRP - Status SS7 Route Print
- STDDP - Status Disk Drive Print
- STEPP - Status Ethernet Port Print
- STHLP - Status Host Link Print
- STIPP - Status IP Print
- STLCP - Status Licensing Print
- STPCP - Status PCM Print
- STRAP - Status Remote Application Server Print
- STRLP - Status Remote SIU Link Print
- STSLP - Status SS7 Link Print
- STSRP - Status SIGTRAN Route Print
- STSTP - SIGTRAN Link Status
- STSYP - Status System Print
- STTDP - Status TCAP Dialog Print
- STTPP - Network Time Protocol Status Print
- STTRP - Status TCAP Resource Print

# Chapter 7: Web-based Management Interface

## 7.1 Overview

The web-based management interface allows the configuration of the higher-level mobile service logic with the SWS system. In addition, it also allows easy access via a browser to much of the status and statistics functionality available in the console-based management interface.

The management interface is accessed by a remote web browser to port **80**.

***Note:*** For example, this will typically be acheived by using the address http://192.168.0.1/ in the address bar.

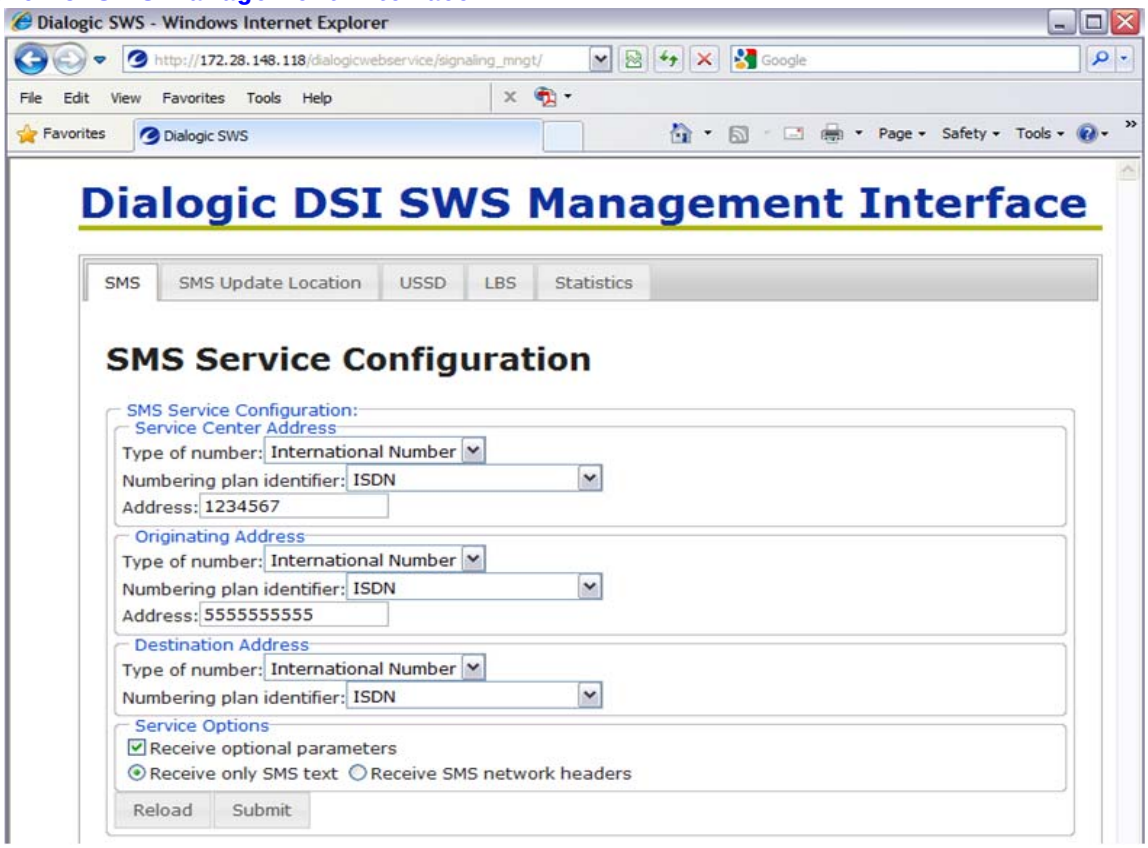
## 7.2 SWS Management

The SWS management interface allows the service-specific parameters of the system to be configured and verified using a web-browser. For each service, i.e., SMS,USSD or location services, there is a different page offering the appropriate configuration options for that service.

Select the SWS Management Interface option to configure and manage the service specific parameters of the system.

Further details of the parameters and services that can be configured are contained on the appropriate web-pages on the system.

**Figure 13. SWS Management Interface**



## 7.3 Web-based status and statistics

Select the `MMI Interface` to access a menu of functions available from the SWS. The functionality is similar to that offered by many of the MMI commands offered via the console-based management interface.

**Figure 14. SWS Web-based status control panel**

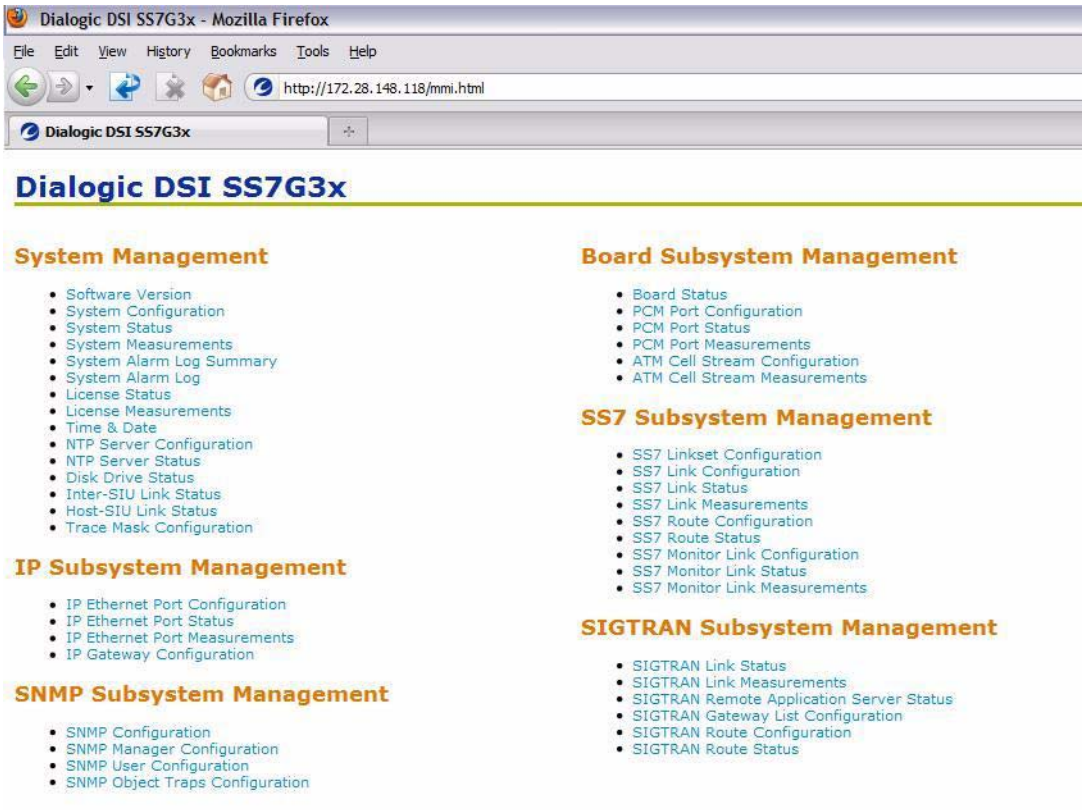
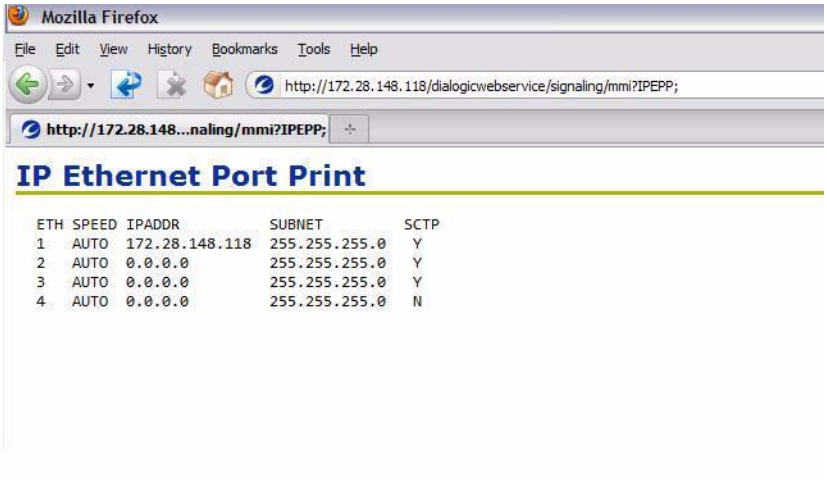


**Figure 15. Example status output**


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://172.28.148.118/dialogicwebservice/signaling/mmi?IPEPP;
http://172.28.148...naling/mmi?IPEPP;
IP Ethernet Port Print
ETH SPEED IPADDR SUBNET SCTP
1 AUTO 172.28.148.118 255.255.255.0 Y
2 AUTO 0.0.0.0 255.255.255.0 Y
3 AUTO 0.0.0.0 255.255.255.0 Y
4 AUTO 0.0.0.0 255.255.255.0 N

# Chapter 8: Configuration

## 8.1 Overview

Initial SWS protocol and physical interface configuration is determined by a text file containing the parameters that are specific to a particular installation. It is necessary for you to modify this file to configure the unit for the desired operation. After this initial configuration, the unit must be restarted before the configuration is applied. Modifications to the configuration require that the text file be updated. If the modifications are to configuration elements capable of dynamic configuration (see Section 9.7, "Dynamic Configuration" on page 173), an update can take place without impact to other configuration elements in the system. If the configuration command cannot be dynamically configured, the SWS requires a restart before the configuration updates can take effect.

Signaling boards are configured using SS7_BOARD commands with the associated PCMs configured using the LIU_CONFIG command.

M2PA Sigtran Links are configured using the STN_LINK command.

The MTP parameters are assigned using the MTP_CONFIG, MTP_NC_CONFIG, MTP_LINKSET, MTP_LINK and MTP_ROUTE commands.

The M3UA parameters are assigned using the STN_NC, STN_LAS, STN_LINK, STN_RAS, STN_RASLIST, STN_ROUTE, STN_RSGLIST and STN_LBIND commands.

The SCCP protocol is configured using the SCCP_CONFIG and SCCP_SSR commands. Subsystems are assigned using SCCP_SSR. Concerned subsystems are configured using SCCP_CONC_SSR.

SCCP Global Title Translations are configured using the SCCP_GTT_PATTERN, SCCP_GTT_ADDRESS and SCCP_GTT commands.

TCAP on the SWS is activated using the TCAP_CONFIG and TCAP_NC_CONFIG commands and may be configured with Dialog groups using the TCAP_CFG_DGRP command.

***Note:*** The definitions of the configuration commands used within this manual are applicable to the versions of software defined in the applicability statement provided in Section 1.4, "Applicability" on page 13. The SWS software continues to support older versions of the commands identified in earlier revisions of this manual unless explicitly stated in the *Release Notes* for the product. It is recommended; however, that the format of commands used is that which is defined in this revision of the manual.

***Note:*** **Attempting to mix, in the same configuration file, lines that use current command formats with lines that use older command formats may give rise to restart errors indicating "inconsistent command format".**

The configuration commands and their parameters are defined in the following sections.

### 8.1.1 Syntax Conventions

In the command description sections of this chapter, the text under the subheading "Syntax" shows a line in the configuration file.

The following conventions apply:

- Each line starts with a keyword and is followed by a number of <parameters>.
- Items in square brackets [ ] are optional.
- The first "*" in a line indicates that the remainder of the line is a comment with no syntactical significance to the operation of the SWS.

Each <parameter> may be:

- A numeric value, specified in decimal format (for example, 1234) or in hexadecimal format by prefixing the value with "0x" (for example, 0x4d2).

- Specified as bit field values, where each bit set to 1 specifies a particular configuration option. The least significant bit is designated bit 0.
- A token, where the possible values are defined in the relevant section.

### 8.1.2 Dynamic Configuration

Dynamic configuration is a feature supported by the SWS providing a user with the ability to add or remove configuration elements on the unit without affecting the status of other elements and without the need for a system restart.

The update to the configuration is achieved by allowing a user to:

1. Modify the configuration file and transfer it into the unit via FTP.
2. Apply an MML command to update the configuration of a circuit group.

This allows the SWS users to escalate their systems by adding or removing resources at runtime without the need to apply a system restart to the unit. In the case that a unit restart is required, the last transferred configuration is the one that is adopted.

See Section 9.7.1, “Config.txt-Based Dynamic Configuration” on page 173 for more information.

## 8.2 Command Sequence

The configuration commands must be entered in the order specified below. The command at the top of the table should be at the start of the configuration file, with the remaining commands following in the order that they appear in the table.

**Table 4. Command Summary**

| Command | Group | Class | Summary |
|---|---|---|---|
| SIU_REM_ADDR | SIU/SWS | O | Set IP address of partner unit in a dual resilient configuration |
| SIU_HOSTS | SIU/SWS | O | Specify the number of host computers attached to the SWS via an RSI interface. Does not limit the number of web-service based clients which can connect. |
| SS7_BOARD | SIU/SWS | M | Configure signaling boards |
| LIU_CONFIG | SIU/SWS | O | Configure T1/E1 PCM network interface trunks |
| STN_NC | STN | M | Define network context and point code type to be used by M3UA |
| STN_LINK | STN | O | Define SIGTRAN links |
| STN_LAS | STN | O | Define a local application server |
| STN_RAS | STN | O | Define a remote application server |
| STN_RASLIST | STN | O | Attach a list of M3UA links to a remote application server |
| STN_ROUTE | STN | O | Define SIGTRAN routes |
| STN_RSGLIST | STN | O | Attach a list of signaling gateways to a SIGTRAN route |
| STN_LBIND | STN | O | Associate the local application server with a remote application server or remote signaling gateway - identifying the route to reach the destination. |
| MTP_CONFIG | MTP | M | Set global MTP operating parameters |
| MTP_NC_CONFIG | MTP | O | Set global MTP parameters for an SS7 Network Context |
| MTP_LINKSET | MTP | M | Define link sets |
| MTP_LINK | MTP | M | Define signaling links |
| MTP2_TIMER | MTP | O | Configure MTP2 (link) timers |

**NOTES:**
1. The Group column defines which part of the system a command configures. All configurations may use the SIU/SWS and MTP commands. The protocol-specific (for example, SCCP etc.) commands should only be used if those software options are licensed and configured in the SWS.
2. Commands shown as “M” are Mandatory for configuring TDM signaling over T1/E1 trunks. Commands shown as “O” are optional.

**Table 4. Command Summary (Continued)**

| Command | Group | Class | Summary |
|---|---|---|---|
| MTP3_TIMER | MTP | O | Configure MTP3 timers |
| MTP_ROUTE | MTP | M | Configure MTP3 routing |
| MTP_USER_PART | MTP | O | Specify a user supplied user part |
| SCCP_CONFIG | SCCP | O | Set SCCP operating parameters |
| SCCP_GTT | SCCP | O | Add a translation to the SCCP global title translation table. |
| SCCP_GTT_ADDRESS | SCCP | O | Define the global title to be used as the primary or backup destination of a translation. |
| SCCP_GTT_PATTERN | SCCP | O | Define the received global title pattern to be matched for a global title translation. |
| SCCP_NC_CONFIG | SCCP | O | Set SCCP operating parameters for Network Context |
| SCCP_SSR | SCCP | O | Configure SCCP sub-system resource |
| SCCP_CONC_SSR | SCCP | O | Configure SCCP concerned sub-system resource |
| TCAP_CONFIG | TCAP | O | Set TCAP operating parameters |
| TCAP_NC_CONFIG | TCAP | O | Set TCAP Network Context operating parameters |
| TCAP_CFG_DGRP | TCAP | O | Define a range of dialogs for a TCAP host |

**NOTES:**
1. The Group column defines which part of the system a command configures. All configurations may use the SIU/SWS and MTP commands. The protocol-specific (for example, SCCP etc.) commands should only be used if those software options are licensed and configured in the SWS.
2. Commands shown as “M” are Mandatory for configuring TDM signaling over T1/E1 trunks. Commands shown as “O” are optional.

## 8.3 Detection of Errors in the Configuration File

The SWS reports errors in the protocol configuration file using the alarm listing available on the management interface. The failure of one or more commands from the file is indicated by a “Configuration failed” alarm report.

If possible, the report also includes a detailed description of the error, as a “Restart error” report, indicating the line number and optionally command type and parameter that are in error. Some examples are provided below:

```
Alarm List (active alarms)
CLA CATEGORY ID  TITLE
5   SYS       0  Parse errors
5   SYS       0  Configuration failed
5   SYS      30  Restart error: SS7_BOARD parameter 2 bad value
5   SYS      42  Restart error: MTP_LINKSET number of parameters
5   SYS      47  Restart error: MTP_LINK unacceptable command
```

The presence of such alarm events in the system indicates that the protocol will not function correctly, hence the operator should consult the section detailing the configuration command in error in order to diagnose and correct the fault before proceeding.

***Note:*** If the Restart error alarm “Inconsistent command format” appears in the alarm list, this indicates that a configuration contains a mix of obsolescent format and current format of statements. To avoid this and to be able to make use of newer features and capabilities introduced since the initial release of the Dialogic® DSI Signaling Server products, you should ensure that:

- MTP_ROUTE statements in your configuration have all documented parameters present (NC is optional however)
- SCCP_LSS is not used - use SCCP_SSR for LSS configuration
- SCCP_RSS is not used - use SCCP_SSR for RSS configuration
- SCCP_RSP is not used - use SCCP_SSR for RSP configuration

## 8.4 SIU/SWS Commands

The SIU/SWS commands include:

- SIU_HOSTS - Number of Hosts
- SIU_REM_ADDR - Other SIU/SWS Ethernet Address

### 8.4.1 SIU_HOSTS – Number of Hosts

#### Synopsis

When this optional command is present, it specifies the number of message-based host computers that the SWS via the will configure and activate. The command also identifies the host backup mode.

***Note:*** SWS systems do not require message-based hosts as they can communicate via the web-services API.

#### Syntax

```
SIU_HOSTS <num_hosts> <backup_mode> <options>
```

#### Examples

```
SIU_HOSTS 4
SIU_HOSTS 4 0
SIU_HOSTS 2 1
```

#### Parameters

The SIU_HOSTS command includes the following parameters:

- **<num_hosts>**
  The number of hosts attached to the SIU/SWS, in the range 0 to 64.
  When <num_hosts> is set to 0 or the SIU_HOSTS command is not present, the SIU/SWS configures the maximum number of hosts available in the system. Only one host (by default host ID 0) is activated and the rest are deactivated, allowing you to dynamically activate or deactivate them using the MNINI and MNINE MML commands.
- **<backup_mode>**
  The backup host algorithm, with of value of 0, 1 or 2 as follows:
  - When this parameter is set to 0 or the SIU_HOSTS command is not present, the SIU/SWS does not employ the backup host mechanism.
  - When set to a value of 1, primary and backup hosts are paired 0-1, 2-3, 4-5 etc. If the link to host 0 fails, messages are sent instead to host 1 and vice versa. When the link recovers, normal routing resumes.
  - When set to a value of 2, primary and backup hosts are paired 0-32, 1-33, 2-34 etc. If the link to host 0 fails, messages are sent instead to host 32 and vice versa. When the link recovers, normal routing resumes.

  The ability to configure backup hosts allows management and/or signaling messages to be redirected to a backup host application in the event of primary host failure. Once the primary host link has been recovered, messages are again sent to it from the SIU/SWS.
  Backup hosts may be used for SCCP operation however, they might not be used in configurations that utilize DTS/DTC. You should ensure that both primary and backup hosts are configured and active.

- Options
  A 32-bit value, each bit of which enables or disables additional configuration options:
  - BIT 0 - When set received MTP-Transfer-Indications will be evenly distributed across all available hosts. The distribution will be in a 'Round-Robin' manner such that the subsequent message gets routed to the next available host
  - All other bits are reserved and should be set to zero.

### 8.4.2 SIU_REM_ADDR – Other SIU/SWS Ethernet Address

#### Synopsis

The SIU_REM_ADDR command defines the network IP address of the other unit when configured in a dual resilient configuration. This command should be omitted if the SWS is not in a dual resilient configuration.

#### Syntax

```
SIU_REM_ADDR <remote_address>
```

#### Example

```
SIU_REM_ADDR 193.195.185.37
```

#### Parameters

The SIU_REM_ADDR command includes the following parameters:

- **<remote_address>**
  The IP address of the “other” SWS/SIU in a dual resilient configuration.

## 8.5 Physical Interface Commands

The physical interface commands include:

- SS7_BOARD - SS7 Board Configuration
- LIU_CONFIG - Line Interface Configuration
- STREAM_XCON - Cross Connect Configuration

### 8.5.1 SS7_BOARD – SS7 Board Configuration

#### Synopsis

The SS7_BOARD command configures a Dialogic® DSI SS7 Network Interface Board and its PCM ports.

***Note:*** An SS7_BOARD configuration command must exist for each SS7 signaling board physically present in the unit.

#### Syntax

```
SS7_BOARD <bpos> <board_type> <flags>
```

#### Examples

```
SS7_BOARD 1 SPCI4     0x0000
SS7_BOARD 2 SPCI4     0x0041
SS7_BOARD 2 SS7HDP    0x0041
```

#### Parameters

The SS7_BOARD command includes the following parameters:

- **<bpos>**
  The board position of the of the signaling board. The valid range is 1 to 3, with board 1 at the bottom of the chassis.
- **<board_type>**
  The board type. Valid values are: SPCI4 and SS7HDP. The Dialogic® DSI SPCI4 and SS7HDP Network Interface Boards have four T1/E1 interfaces. The SPCI4 boards support up to four SS7 signaling links, while the SS7HDP board supports up to 64 SS7 signaling links.
- **<flags>**
  A 16-bit value used to configure run-time configuration options. Bits 6 and 0 are used as detailed in the following table:

| Bit 6 | Bit 0 | Clocking Mode |
|---|---|---|
| 0 | 0 | T1/E1 clocks are generated from the local oscillator on this board. The board is isolated from the internal telephony bus and no interconnection between signaling boards is permitted. |
| 0 | 1 | T1/E1 clocks are recovered from the highest priority T1/E1 port on this board and used as the output clock for all other ports on this board. The board is isolated from the internal telephony bus and no interconnection between signaling boards is permitted. The highest priority clock source is taken from the first configured PCM and then the next highest priority from subsequent configured ports. |
| 1 | 0 | Reserved – do not use. |
| 1 | 1 | T1/E1 clocks are shared between all boards. The clock is recovered from the highest priority T1/E1 interface in the system and used for all other T1/E1 clock outputs. The board is connected (using the internal telephony bus) to all other boards that use this setting and full interconnection between signaling boards is supported. If the highest priority clock source is not currently valid then the next highest priority input is automatically selected. The priority of each T1/E1 input is controlled using the **<syncpri>** parameter in the LIU_CONFIG command. |

All other bits in the **<flags>** parameter are reserved and should be set to zero.

### 8.5.2 LIU_CONFIG – Line Interface Configuration

#### Synopsis

The LIU_CONFIG command is used to configure the PCM format used by the signaling boards.

#### Syntax

For Dialogic® DSI SS7HD Network Interface Boards:

```
LIU_CONFIG <port_id> <pcm> <liu_type> <line_code> <frame_format> <crc_mode> <syncpri> <build_out>
<slave_port_id> <flags>
```

For Dialogic® DSI SPCI4 Network Interface Boards:

```
LIU_CONFIG <port_id> <pcm> <liu_type> <line_code> <frame_format> <crc_mode> <syncpri> <reserved>
<slave_port_id> <flags>
```

#### Example

```
LIU_CONFIG 0 1-3 5 1 1 1 0 0 0 0x0000
```

#### Parameters

The LIU_CONFIG command includes the following parameters:

- **<port_id>**
  Logically identifies the PCM port in the SWS range. The port_id should be unique within the system and in the range 0 to 11.
- **<pcm>**
  Identifies the physical interface to the system for LIU. It is a compound parameter, made up of board position and LIU interface number, for example, 2-4. The boards on the Signaling Server are numbered from 1 to 3, with board 1 at the bottom of the chassis. Valid values for the interface on the board are 1 to 4 for the SPCI4 and SS7HDP boards.
- **<liu_type>**
  Specifies the physical type of interface required according to the following table. Note that this must be selected by you to be appropriate for the actual hardware fitted otherwise, an error status is returned. This parameter must be set to one of the following values:

| Value | Meaning |
|---|---|
| 4 | T1 |
| 5 | E1 balanced |
| 6 | E1 high-impedance (for monitoring applications) |
| 7 | T1 high-impedance (for monitoring applications) |

***Note:*** Use of the Buildout parameter is not relevant when high impedance is configured on a PCM. Users are required to set it to a value of 0 for when either E1 high-impedance (6) or T1 high-impedance (7) is configured on the PCM.

- **<line_code>**
  The line coding technique. The following table shows the permitted values and their meaning.

| Value | Description |
|---|---|
| 1 | HDB3 (E1 only) |
| 2 | AMI with no Zero Code Suppression |
| 3 | AMI with Zero Code Suppression. The appropriate bit in the clear_mask parameter may be set to disable Zero Code Suppression for individual timeslots if required. (T1 only) |
| 4 | B8ZS (T1 only) |

- **<frame_format>**
  The frame format. The following table shows the permitted values and their meaning.

| Value | Description |
|---|---|
| 1 | E1 double frame (E1 only) |
| 2 | E1 CRC4 multiframe (E1 only) |
| 4 | D3/D4 (Yellow alarm = bit 2 in each channel; T1 only) |
| 7 | ESF (Yellow alarm in data link channel; T1 only) |
| 10 | Unstructured high speed links |

- **<crc_mode>**
  The Cyclic Redundancy Check (CRC) mode of operation. The following table shows the permitted values and their meaning.

| Value | Description |
|---|---|
| 1 | CRC generation disabled |
| 2 | CRC4 enabled (frame_format must be set to 2) |
| 3 | CRC4 compatibility mode (E1 only) |
| 4 | CRC6 enabled (T1 only) |
| 5 | CRC4 G.706 compatible mode (frame_format must be set to 2)<br>**NOTES:**<br>1. Out of CRC4-multiframe E-Bits are transmitted as zeroes.<br>2. This value is supported on SS7HDP boards only. |

- **<syncpri>**
  Specifies the relative clock priority of individual T1/E1 interfaces. This parameter allows you to prevent the interface being used for clock recovery (syncpri=0) or select a number in the range 1 to 32, where 1 is the highest priority and 32 is the lowest. The use of the same value for multiple interfaces is permitted, in which case the lowest numbered port on the lowest numbered board takes the highest priority. The parameter should be specified when the internal telephony bus is activated by flags in the SS7_BOARD command. When the internal telephony bus is not activated (see SS7_BOARD above) this parameter should be zero.
- **<build_out>**
  Specifies the range of “build out” settings for a T1 interface. The parameter is required for SS7HDP boards. The following table shows the permitted values and their meaning.

| Value | Description | Valid For |
|---|---|---|
| 0 | E1 setting (default) | liu_type = 5 |
| 1 | T1 short haul, 0 to 110 ft. (default) | liu_type = 4 |
| 2 | T1 short haul, 0 to 110 ft. (same as value=1) | |
| 3 | T1 short haul, 110 to 220 ft. | |
| 4 | T1 short haul, 220 to 330 ft. | |
| 5 | T1 short haul, 330 to 440 ft. | |
| 6 | T1 short haul, 440 to 550 ft. | |
| 7 | T1 short haul, 550 to 600 ft. | |
| 8 | T1 long haul LB0 (-0db) | |
| 9 | T1 long haul LB0 (-7.5db) | |
| 10 | T1 long haul LB0 (-15db) | |
| 11 | T1 long haul LB0 (0db, TR62411) | |

  For SPCI4 boards, the parameter is unused (reserved) and should be set to 0.
- **<slave_port_id>**
  Identifies an optional slave port where alarm conditions occuring on this LIU will be mapped to AIS on the slave port. The slave port is typically used in conjunction with the STREAM_XCON command which

maps timeslots from one LIU through to another “slave” LIU. When bit 0 of the flags field is set, the slave_port_id must be set to a configured port that has not been previously configured as a slave port on another LIU. When bit 0 is not set, the slave_port_id field should be set to 0.

- **<flags>**

  A 16-bit value used to configure run-time configuration:

  — Bit 0 indicates whether this LIU has an associated “slave” LIU. When set, the slave_port_id must be set to a configured port that has not been previously configured as a slave port on another LIU.

  All other bits in the <flags> parameter are reserved and should be set to zero.

### 8.5.3 STREAM_XCON – Cross Connect Configuration

#### Synopsis

The STREAM_XCON command controls the cross connect switch on the signaling boards, enabling the cross-connection of timeslots between the two PCM ports on each signaling board or a fixed pattern to be generated on specified timeslots. The PCM ports on a board are referenced by a fixed logical stream number.

#### Syntax

```
STREAM_XCON <bpos> <stream_a> <stream_b> <mode> <ts_mask> <pattern>
```

#### Example

```
STREAM_XCON 3 2 3 3 0xfffefffe 0
```

#### Parameters

The STREAM_XCON command includes the following parameters:

- **<bpos>**
  The board position of the cross connect switch to be controlled. There must be a valid board at this position (previously defined by an SS7_BOARD command).
- **<stream_a>**
  A reference to the 2 Mbps stream for the output of the connection or the fixed data pattern. There must be a valid PCM port at this position (previously defined by a LIU_CONFIG command). Valid values are:

| Board Type | Stream | T1/E1 interface |
|---|---|---|
| SPCI4, SS7HDP | 0 | L1 |
| | 1 | L2 |
| | 2 | L3 |
| | 3 | L4 |

- **<stream_b>**
  A reference to the 2 Mbps stream for the input of a simplex connection (mode 2) or one half of a duplex cross connection (mode 3). In other modes, this field should be set to zero.
  There must be a valid PCM port at this position (previously defined by a LIU_CONFIG command). For valid values, see the table in the <stream_a> parameter description above.
- **<mode>**
  Indicates the requested cross connect switch function according to the following table.

| Mode | Function |
|---|---|
| 1 | Set a fixed pattern specified by <pattern> on the output timeslot(s). |
| 2 | Connect the input timeslot to the output timeslot. |
| 3 | Duplex cross-connect the input and output timeslot. |

- **<ts_mask>**
  A 32-bit mask specifying the timeslots to apply the cross connect or pattern to. Each bit corresponds to a timeslot in the input/output stream. Bit 0 (the least significant bit) corresponds to timeslot number 0. To apply this command to a timeslot, the corresponding bit must be set to one.
  - E1 interfaces have 32 timeslots *numbered 0 to 31*. Timeslot 0 is used for frame alignment and timeslot 16 is generally used for signaling or is empty. Hence the normal SWS configuration is to cross connect timeslots 1 to 15 and 17 to 31 between the two ports on each signaling board by setting the ts_mask value to 0xfffefffe.
  - T1 interfaces have 24 timeslots, *numbered 1 to 24*. To cross connect all the timeslots on a T1 interface between the two PCM ports on a signaling board, the ts_mask value 0x1fffffe should be used.

  In duplex mode both PCM ports should have been previously configured under the same type of PCM connector E1 or T1.

- <**pattern**>
  One byte of fixed data to output in pattern mode (mode 1) on the output stream/timeslot. In other modes, this parameter should be set to zero.

## 8.6 MTP Commands

The MTP commands include:

- MTP_CONFIG - Global MTP Configuration
- MTP_NC_CONFIG - Network Context MTP Configuration
- MTP_LINKSET - MTP Link Set
- MTP_LINK - MTP Signaling Link
- MTP2_TIMER - MTP2 Timer Configuration
- MTP3_TIMER - MTP3 Timer Configuration
- MTP_ROUTE - MTP Route
- MTP_USER_PART - MTP User Part

### 8.6.1 MTP_CONFIG – Global MTP Configuration

#### Synopsis

The MTP_ CONFIG command defines the global configuration parameters for MTP when existing in a single network or for Network Context 0 (NC0) when existing in multiple Network Contexts.

#### Syntax

```
MTP_CONFIG <reserved1> <reserved2> <options>
```

#### Example

```
MTP_CONFIG 0 0 0x0000
```

#### Parameters

The MTP_CONFIG command includes the following parameters:

- <**reserved1**>
  Reserved for future use. This parameter should be set to zero.
- <**reserved2**>
  Reserved for future use. This parameter should be set to zero.
- <**options**>
  A 32-bit value, each bit of which enables or disables additional configuration options:
  - Bit 0 defines the operation of MTP3 when a message is received from the SS7 network with a Destination Point Code (DPC) different from the local point code configured for the link set. When set to zero, these messages are discarded. When set to 1, all received messages are processed regardless of dpc value. This bit is normally set to zero.
  - Bit 1 defines the operation of MTP3 when a message is received from the SS7 network with a sub-service field (ssf) value different from the ssf value configured for the link set. When set to zero, these messages are discarded. When set to 1, all received messages are processed regardless of ssf value. This bit is normally set to zero.
  - Bit 3 determines the behavior when a message is received from the SS7 network for a User Part that has not been configured. If set to 1, a User Part Unavailable (UPU) message is issued to the network, zero prevents the UPU from being issued. This bit is normally set to zero.
  - Bit 6 controls the operation of the Signaling Route Set Test mechanism. Normally, when a remote signaling point becomes unavailable, a periodic Signaling Route Set Test message is issued in order to provide that subsequent availability of the signaling point is detected. Setting this bit to 1 disables the sending of this message. This bit is normally set to zero.
  - Bit 8 selects between ITU-T (CCITT) and ANSI operation. If set to 1, the MTP operates in accordance with ANSI T1.111, if set to 0, the MTP operates in accordance with the ITU-T (CCITT) Q.700 series recommendations.

— Bit 9 selects between 14/16-bit point codes and 24-bit point codes:
- When set to 0, 14-bit or 16-bit point codes are selected (see also Bit 20).
- When set to 1, 24-bit point codes are selected.

***Note:*** Bit 9 must always be set to 1 for ANSI operation.

— Bit 10 is used to enable multiple congestion states.

***Note:*** Bit 10 must always be set to 1 for ANSI operation.

— Bit 11 is used to enable Multiple Message Priority operation.

***Note:*** Bit 11 must always be set to 1 for ANSI operation.

— Bit 16 is used to control the usage of the **hdr->id** field of MTP Transfer Indication messages:
- When set to 0, the **id** field contains the User Part Reference (or Service Indicator), this is primarily useful for backward compatibility.
- When set to 1, the **id** field provides an indication of the MTP Label Format used in the parameter area. This is the recommended setting for all new designs.

***Note:*** Bit 16 must to be set to 1 for the mixed network ISUP configuration.

— Bit 17 controls how received Transfer Controlled and Signaling Route Set Congestion Messages that are not destined for the local point code are processed:
- When set to 0, messages are discarded.
- When set to 1, messages are sent to fixed module_id 0x0a on the host.

— Bit 18 controls MTP3 operation on detection of Remote Processor Outage (RPO):
- When set to 0, on detection of RPO, the signaling link is taken out of service and restoration commences. This setting is useful for backward compatibility.
- When set to 1, normal setting, RPO is handled in accordance with the ITU-T 1992 (and later) recommendations."

— Bit 19 is used when MTP3 is operating in dual mode to control which bit of the Sub-Service Field is used to flag messages that have been received by one MTP3 and are being conveyed to the dual module over the inter-MTP3 link set.

o 0 - Normal setting; sub-Service Field bit 2 is modified.

o 1 - Alternative setting; sub-Service Field bit 0 is modified.

— Bit 20 is used to select between 14-bit point codes and 16-bit point codes. It is only significant when 24-bit point codes are **not** selected (that is, when bit 9 is set to 0):
- When set to 0, 14-bit point codes are selected.
- When set to 1, 16-bit point codes are selected.

— Bit 21 is used to activate Japan-specific MTP3 operation:
- When set to 0, normal setting, Japan-specific functionality is disabled.
- When set to 1, Japan-specific functionality is enabled.

— Bit 22 the handling of received Route Set Test Messages. It should only be set if bit 17 is also set:
- Normal operation; Route Set Test messages processed by MTP3.
- When set to 1, messages are sent to fixed module_id 0x0a on the host.

***Note:*** For correct Japan-specific operation, you should also select 16-bit point codes by setting bit 20 as well as bit 21.

All other bits are reserved and should be set to zero.

### 8.6.2 MTP_NC_CONFIG – Network Context MTP Configuration

#### Synopsis

The MTP_NC_CONFIG command defines the global configuration parameters for MTP existing in an additional SS7 Network Context to that identified by the MTP_CONFIG command.

#### Syntax

```
MTP_NC_CONFIG <nc_id> <options>
```

#### Example

```
MTP_NC_CONFIG NC1  0x0000
```

### Parameters

The MTP_NC_CONFIG command includes the following parameters:

- **<nc_id>**
  SS7 Network Context. This parameter uniquely identifies the SS7 network that MTP is being configured for. Supported values are: NC1, NC2 and NC3.
- <**options**>
  A 32-bit value, each bit of which enables or disables additional configuration options:
  - — Bit 0 defines the operation of MTP3 when a message is received from the SS7 network with a Destination Point Code (DPC) different from the local point code configured for the link set. When set to zero, these messages are discarded. When set to 1, all received messages are processed regardless of DPC value. This bit is normally set to zero.
  - — Bit 1 defines the operation of MTP3 when a message is received from the SS7 network with a sub-service field (ssf) value different from the ssf value configured for the link set. When set to zero, these messages are discarded. When set to 1, all received messages are processed regardless of ssf value. This bit is normally set to zero.
  - — Bit 3 determines the behavior when a message is received from the SS7 network for a User Part that has not been configured. If set to 1, a User Part Unavailable (UPU) message is issued to the network. If set to zero, UPU messages are not issued. This bit is normally set to zero.
  - — Bit 6 controls the operation of the Signaling Route Set Test mechanism. Normally, when a remote signaling point becomes unavailable, a periodic Signaling Route Set Test message is issued to provide that subsequent availability of the signaling point is detected. Setting this bit to 1 disables the sending of this message. This bit is normally set to zero.
  - — Bit 8 selects between ITU-T (CCITT) and ANSI operation. If set to 1, the MTP operates in accordance with ANSI T1.111. If set to 0, the MTP operates in accordance with the ITU-T (CCITT) Q.700 series recommendations.
  - — Bit 9 selects between 14/16-bit point codes and 24-bit point codes:
    - When set to 0, 14-bit or 16-bit point codes are selected (see also Bit 20).
    - When set to 1, 24-bit point codes are selected.

  ***Note:*** Bit 9 must always be set to 1 for ANSI operation.

  - — Bit 10 is used to enable multiple congestion states.

  ***Note:*** Bit 10 must always be set to 1 for ANSI operation.

  - — Bit 11 is used to enable Multiple Message Priority operation.

  ***Note:*** Bit 11 must always be set to 1 for ANSI operation.

  - — Bit 16 is used to control the usage of the **hdr->id** field of MTP Transfer Indication messages:
    - When set to 0, the **id** field contains the User Part Reference (or Service Indicator), this is primarily useful for backward compatibility.
    - When set to 1, the **id** field provides an indication of the MTP Label Format used in the parameter area. This is the recommended setting for all new designs.

  ***Note:*** Bit 16 must to be set to 1 for the mixed network ISUP configuration.

  - — Bit 17 controls how received Transfer Controlled and Signaling Route Set Congestion Messages that are not destined for the local point code are processed:
    - When set to 0, messages are discarded.
    - When set to 1, messages are sent to fixed module_id 0x0a on the host.
  - — Bit 18 controls MTP3 operation on detection of Remote Processor Outage (RPO):
    - When set to 0, on detection of RPO, the signaling link is taken out of service and restoration commences. This setting is useful for backward compatibility.
    - When set to 1, which is the normal setting, RPO is handled in accordance with the ITU-T 1992 (and later) recommendations."
  - — Bit 20 is used to select between 14-bit point codes and 16-bit point codes. It is only significant when 24-bit point codes are **not** selected (that is, when bit 9 is set to 0):
    - When set to 0, 14-bit point codes are selected.
    - When set to 1, 16-bit point codes are selected.

— Bit 21 is used to activate Japan-specific MTP3 operation:
- When set to 0, normal setting, Japan-specific functionality is disabled.
- When set to 1, Japan-specific functionality is enabled.

— Bit 22 the handling of received Route Set Test Messages. It should only be set if bit 17 is also set:
- Normal operation; Route Set Test messages processed by MTP3.
- When set to 1, messages are sent to fixed module_id 0x0a on the host.

***Note:*** For correct Japan-specific operation, you should also select 16-bit point codes by setting bit 20 as well as bit 21.

All other bits are reserved and should be set to zero.

### 8.6.3 MTP_LINKSET – MTP Link Set

#### Synopsis

The MTP_LINKSET command defines link sets.

#### Syntax

```
MTP_LINKSET [<nc_id>] <linkset_id> <adjacent_spc> <num_links> <flags> <local_spc> <ssf>
```

#### Example

```
MTP_LINKSET 0 321 2 0x0000 320 0x8
MTP_LINKSET NC0 0 321 2 0x0000 320 0x8
```

#### Parameters

The MTP_LINKSET command includes the following parameters:

- **<nc_id>**
  SS7 Network Context. The Network Context together with a Signaling Point Code (SPC) uniquely identify an SS7 node by indicating the specific SS7 network it belongs to. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2 or NC3.
- **<linkset_id>**
  The logical identity of the link set, in the range 0 to one less than the maximum number of link sets supported. This ID is used in other commands for reference.
- **<adjacent_spc>**
  The point code of the adjacent signaling point.
- **<num_links>**
  The (maximum) number of links that are allocated to the link set. The valid range is 1 to 16.
- **<flags>**
  A 16-bit value used to specify run time options:
  — Bit 3 when set enables restart procedures for this link set.
  — Bit 15 assigns special functionality to a link set for use in inter-SWS communication. For a normal link set conforming to the SS7 specifications, this bit must be set to 0.

  ***Note:*** Bit 15 must be set for the inter-SWS link set between SWSA and SWSB in a dual resilient configuration.

  — All other bits are reserved and should be set to zero.
- <**local_spc**>
  The local signaling point code for this link set.
- <**ssf**>
  The value to be used in the sub-service field of level 3 messages for this link set. The valid range is 0 to 15. For ANSI operation, the two least significant bits (B and A) must be set to 1 to assign a message priority of 3 to all MTP3 generated messages. The remaining two bits are the network indicators (bits C and D).

***Note:*** For correct SWS operation, the adjacent point code must also appear in an MTP_ROUTE declaration.

### 8.6.4 MTP_LINK – MTP Signaling Link

#### Synopsis

The MTP_LINK command configures signaling links, specifying the physical channel that the link will use.

#### Syntax

```
MTP_LINK <link_id> <linkset_id> <link_ref> <slc> <bpos> <blink> <bpos2> <stream> <timeslot> <flags>
```

#### Example

```
MTP_LINK 0 0 0 0 1 2 1 2 01 0x0006
```

#### Parameters

The MTP_LINK command includes the following parameters:

- <**interface mode**>
  <interface_mode> identifies the interface type for signaling links.
  The interface mode should be set to one of the following values:

| Interface_mode | Description |
|---|---|
| TDM | Single timeslot signaling link |
| E1_HSL | Unstructured E1 HSL operation.<br>***Note***: LIU frame_format must be set to 10. |
| T1_HSL | Unstructured T1 HSL operation.<br>***Note***: LIU frame_format must be set to 10. |
| E1_FRAMED | Framed 31 timeslot E1 operation |
| T1_FRAMED | Framed 24 timeslot T1 operation |
| E1_PCM | Structured 30 timeslot E1 operation (timeslots 0 and 16 are used for signaling) |

  The interface_mode value must be consistent with the liu_type and frame_format values of the LIU_CONFIG command.
- **<link_id>**
  The link's unique logical link identity within the SWS. It must be in the range 0 to one less than the maximum number of signaling links supported.
- **<linkset_id>**
  The logical identity of the link set to which the link belongs. The link set must already have been configured using the MTP_LINKSET command.
- **<link_ref>**
  The logical identity of the signaling link within the link set. It should be in the range 0 to 15. This is usually be the same value set for the <**slc**> parameter below.
- **<slc>**
  The signaling link code for the signaling link. This must be unique within the link. The valid range is 0 to 15.
- **<bpos>**
  The board identifier of the signaling processor allocated for this signaling link. The board must already have been configured using the SS7_BOARD command.
  Set to 0 if the MTP link is associated with an M2PA link.
- **<blink>**
  The index of the logical signaling processor (SP) channel (on the board) allocated for this signaling link.
  — For Dialogic® DSI SPCI4 Network Interface Boards that have a single processor supporting 4 signaling links, the blink parameter may be written as a single value in the range 0 to 3.

Alternatively, it may be written as a compound parameter (as described below for the SS7HD board), but for these board types, the processor number must be 0 and the channel is in the range 0 to 3.

— For the Dialogic® DSI SS7HDP Network Interface Board that has two signaling processors with each processor supporting up to 32 signaling links, the blink parameter is a compound parameter of the form x-y, where x represents the processor (a value of 0 or 1) and y represents the SS7 signaling processor channel within the processor (a value in the range 0 to 31).

— When the SS7 link is to be conveyed over M2PA, the blink parameter identifies the SNLINK (link_id).

— For HSL links the signaling processor channel of the <blink> parameter must be set to 0. Only values of 0-0 and 1-0 are permitted. On an SS7HDP board, a single processor cannot be configured for both HSL and TDM links. Different processors on the same SS7HDP board can be used individually for HSL and non-HSL operation.

- **<bpos2>**

  The board identifier of the stream from which the signaling is to be inserted. The board must have been configured using the SS7_BOARD command. This parameter must be used when setting up link connections across boards. When the SS7_BOARD is configured to be isolated from the internal telephony bus, **<bpos2>** must equal **<bpos>**.

- **<stream>**

  A reference to the logical PCM highway from which the signaling processor is to insert the signaling. This must be in the range 0 to 3. Set to 0 if the MTP link is associated with an M2PA link.

  Valid values are shown in the following table:

| Network Inteface Board Type | Stream | Port | Connector |
|---|---|---|---|
| Dialogic® DSI SPCI4<br>Dialogic® DSI SS7HDP | 0 | 1 | RJ45 L1 |
| | 1 | 2 | RJ45 L2 |
| | 2 | 3 | RJ45 L3 |
| | 3 | 4 | RJ45 L4 |

- **<timeslot>**

  The timeslot on the <stream> that should be used for signaling. For a T1 port, the range is 1 to 24. For an E1 port, the valid range is 1 to 31. The timeslot must not have been previously assigned another MTP or Monitor link. Set to zero if the MTP link is associated with an M2PA link.

  For HSL links, the timeslot parameter should be set to 0xff to indicate that the link is attached to an LIU configured with the LIU_CONFIG command. HSL signaling might not use timeslots already configured for signaling or data.

- **<flags>**

  A 32-bit value, each bit enabling or disabling additional run-time options:

  — Bit 0 is used to signify “override automatic selection of proving period”. When set to 1, bit 3 is used to determine whether to use the EMERGENCY or NORMAL proving procedures. If set to 0, the appropriate proving period in accordance with the SS7 protocol is used.

  — Bit 1 when set to 1 causes a signaling link test to be performed on link activation/restoration. If set to 0, a signaling link test is not performed. This bit should normally be set to 1.

  — Bit 2 when set to 1 enables a periodic signaling link test. When set to 0, periodic signaling link tests are not automatically performed. This bit should normally be set to 1.

  — Bit 3 when set to 1 forces NORMAL proving, otherwise EMERGENCY proving is used. If Bit 0 is set to 0, then the appropriate proving period in accordance with the SS7 protocol is used and Bit 3 has no influence.

  — Bit 7 selects the LSSU length indicator. If set to 1, the unit sends two octet LSSU messages. If set to 0, the unit sends one octet LSSU messages.

  — Bit 8 selects the error correction method used by this link. If set to 1, Preventative Cyclic Retransmission (PCR) is used. If set to 0, the basic error correction method is used. PCR is typically only used over transmission links where the transmission delay is large (such as satellite links).

— Bits 10 and 11 select either 64, 56, or 48 Kbps operation, and are used when a link operates over a T1 or E1 timeslot. Use of these bits is as follows:

| Bit 11 | Bit 10 | Rate | Timeslot Usage |
|---|---|---|---|
| 0 | 0 | 64 Kbps | Set both to zero for E1_HSL and T1_HSL operation. HSL framed operation uses these bits in a similar manner to single timeslot signaling to select 64 Kbps, 56 Kbps or 48 Kbps operation that applies to all timeslots within the HSL link. |
| 0 | 1 | 48 Kbps | bits 7&8 not used |
| 1 | 1 | 56 Kbps | bit 8 not used |

— Bit 12 –sequence number length. Set to 1 the HSL signaling link will use a 12-bit sequence number. Set to 0, the HSL signaling link will use a 7-bit sequence number. 12 bit sequence numbers might not be used for LSL links.

— Bit 31, when set to 1, associates the SS7 link with an M2PA link as identified by the BLINK parameter. bpos, stream and timeslot should all be set to zero. An SS7 link can only be associated with one M2PA link and 2 SS7 links cannot identify the same M2PA link.

— All other bits are reserved and should be set to zero.

### 8.6.5 MTP2_TIMER – MTP2 Timer Configuration

#### Synopsis

The MTP2_TIMER command provides the ability to configure the MTP2 protocol timers from the configuration file.

#### Syntax

```
MTP2_TIMER [<nc_id>] <table_id> <timer_id > <value>
```

#### Example

```
MTP2_TIMER 0 T4N 550
MTP2_TIMER NC1 0 T4N 550
```

#### Parameters

The MTP2_TIMER command includes the following parameters:

- **<nc_id>**
  SS7 Network Context. This parameter uniquely identifies the SS7 network that the MTP2 timer is being configured for. Supported values are: NC0, NC1, NC2 and NC3. When the parameter is not present, a value of NC0 is assumed.
- **<table_id>**
  Reserved for future use and must always be set to zero.
- **<timer_id>**
  A text identifier for the timer to be configured. It should be set to one of the following:
  T1, T2, T3, T4N, T4E, T5, T6, or T7
- **<value>**
  The timer value in multiples of tenths of a second (100 ms).
  Any timers not configured continue to be set to the values shown in the following table. ITU-T or ANSI selection is made by setting the value of the MTP_CONFIG options parameter.

| MTP2 Timer | ITU-T 64k mode | ITU-T 48k mode | ANSI 64k mode | ANSI 56k mode | HSL |
|---|---|---|---|---|---|
| T1 | 45 s | 45 s | 13 s | 13 s | 300 s |
| T2 | 30 s | 30 s | 23 s | 23 s | 30 s |
| T3 | 1.2 s | 1.2 s | 11.5 s | 11.5 s | 1.2 s |
| T4N | 8.2 s | 2.3 s | 2 s | 2.3 s | 30 s |
| T4E | 500 ms | 600 ms | 500 ms | 600 ms | 500 ms |

| MTP2 Timer | ITU-T 64k mode | ITU-T 48k mode | ANSI 64k mode | ANSI 56k mode | HSL |
|---|---|---|---|---|---|
| T5 | 100 ms | 100 ms | 100 ms | 100 ms | 100 ms |
| T6 | 5.5 s | 5.5 s | 5.5 s | 5.5 s | 5.5 s |
| T7 | 1.7 s | 1.7 s | 1.5 s | 1.5 s | 1.5 s |

***Note:*** The SWS does not perform checks on MTP2 timer values.

### 8.6.6 MTP3_TIMER – MTP3 Timer Configuration

#### Synopsis

The MTP3_TIMER command provides the ability to configure the MTP3 protocol timers from the configuration file.

#### Syntax

```
MTP3_TIMER [<nc_id>] <table_id> <timer_id > <value>
```

#### Example

```
MTP3_TIMER 0 T4 12
MTP3_TIMER NC1 0 T4 12
```

#### Parameters

The MTP3_TIMER command includes the following parameters:

- **<nc_id>**
  SS7 Network Context. This parameter uniquely identifies the SS7 network that the MTP3 Timer is being configured for. Supported values are: NC0, NC1, NC2 and NC3. When the parameter is not present, a value of NC0 is assumed.
- **<table_id>**
  Reserved for future use and must always be set to zero.
- **<timer_id>**
  A text identifier for the timer to be configured. It should be set to one of the following:
  T1, T2, T3, T4, T5, T6, T10, T12, T13, T14, T15, T16, T17, T22, T23 T24, SLTC1 or SLTC2.

- **<value>**
  The timer value in multiples of tenths of a second (100ms). Any timers not configured continue to be set to the values shown in the following table. ITU-T or ANSI selection is made by setting the value of the MTP_CONFIG options parameter.

| MTP3 Timer | ITU-T mode | ANSI mode |
|---|---|---|
| T1 | 1 s | 1 s |
| T2 | 1.5 s | 1.5 s |
| T3 | 1 s | 1 s |
| T4 | 1 s | 1 s |
| T5 | 1 s | 1 s |
| T6 | 1s | 1 s |
| T10 | 45 s | 45 s |
| T12 | 1.2 s | 1.2 s |
| T13 | 1.2 s | 1.2 s |
| T14 | 3 s | 2.5 s |
| T15 | 3 s | 2.5 s |
| T16 | 1.8 s | 1.8 s |
| T17 | 1 s | 1 s |
| T22 | 270 s | 270 s |
| T23 | 270 s | 270 s |
| T24 | 500 ms | 500 ms |
| SLTC T1 | 7 s | 7 s |
| SLTC T2 | 30 s | 30 s |

***Note:*** T9 is not used on the SWS.

***Note:*** The SWS does not perform checks on MTP3 timer values.

***Note:*** MTP timers not specified in this table are not configurable; they well be set to their specific ITU or ANSI default value.

### 8.6.7 MTP_ROUTE – MTP Route

**Synopsis**

The MTP_ROUTE command configures a route for use with one of more user parts. Each remote signaling point must have a corresponding MTP_ROUTE entry in the configuration file, which must be entered after the MTP_LINKSET command. Using the **<flags>** and **<second_ls>** parameters, this command can configure a combined link set to a remote Destination Point Code (DPC).

An MTP route exists within a particular Network Context and might not use link sets operating within differing Network Contexts.

MTP routes can be designated as “default” routes and can be used to convey traffic for multiple destinations without the need to configure each DPC as an explicit MTP route. Typically, this is useful when a signaling point connects simply to a single STP or a mated pair of STPs and all traffic can be sent to the STP irrespective of the current network status.

Two types of default route are supported, one associated with a “real” DPC. In this case, the (default) route is deemed to be accessible whenever the specified DPC is accessible. The other associated with a “pseudo” DPC which is a point code that does not exist within the network (for example, zero). In this case the (default) route is deemed to be accessible as soon as the link sets within the route are available.

A maximum of one default route for each supported Service Indicator (or user part) is permitted.

***Note:*** The MTP_ROUTE command must be used for each destination point code to be accessed *including* the adjacent point code. There may be only one MTP_ROUTE command for each destination.

***Note:*** **Attempting to mix, in the same configuration file, lines that use current command formats with lines that use older command formats may give rise to restart errors indicating "inconsistent command format".**

### Syntax

```
MTP_ROUTE [<nc_id>] <route_id> <dpc> <linkset_id> <user_part_mask> <flags> <second_ls> <reserved>
```

### Example

```
MTP_ROUTE 1 567 1 0x0008 0x0000 0 0
MTP_ROUTE NC0 1 567 1 0x0008 0x0000 0 0
```

### Parameters

The MTP_ROUTE command includes the following parameters:

- **<nc_id>**
  SS7 Network Context. This parameter identifies the SS7 network in which the route exists. The Network Context must match that of the link set(s) in the route. Supported values are: NC0, NC1, NC2 or NC3. When the parameter is not present, a value of NC0 is assumed.
- <**route_id**>
  A unique value in the range 0 to 128 used to identify the MTP route.
- **<dpc>**
  The remote destination signaling point code for the route.
- **<linkset_id>**
  The logical identity of the link set, in the range 0 to one less than the maximum number of link sets supported. This value is set for each configured link set in the MTP_LINKSET command.
- **<user_part_mask>**
  A 16-bit value with bit n (in the range 3 to 15) set to allow the route to be used for messages with Service Indicator (SI) n. For each user part supported, the bit corresponding to the Service Indicator for that user part should be set. For example, to enable SCCP routing (which uses an SI of 3) a value of 0x0008 should be used. To enable both SCCP (3) and ISUP (5) a value of 0x0028 should be used.
- **<flags>**
  A 16-bit value that provides additional options:
  - — Bit 0 is set to 1 to enable the use of the <second_ls> parameter.
  - — Bit 1 is set to 1 to cause traffic sent towards the remote signaling point to be shared between the two link sets <linkset_id> and <second_ls>. If set to 0, all traffic sent towards the remote signaling point is normally sent using the link set specified by <linkset_id>, unless this link set fails, in which case the traffic uses the alternative link set <second_ls>. Loadsharing should not be configured if one of the link sets is used between a pair of SWSs in a dual SWS configuration.
  - — Bit 2 is set to 1 to indicate a default route. Messages for any DPC that is not explicitly configured use this route.
  - — Bit 3 is set to 1 to indicate that the DPC associated with this route is not a real DPC within the network. The route is considered available as soon as the link sets within the route are available.

  ***Note:*** When bit 3 is set, bit 2 should also be set.

  - — Bit 5 is set to 1 to disable the Route Test procedure for this route. Typically, this bit should be set to zero. However, in the case of a "pseudo" DPC route, it is essential to set this bit to 1 to prevent RST messages being issued.
  - — All other bits must be set to zero.
- **<second_ls>**
  The logical identity of the second link set in the combined link set.

- **<reserved>**
  Reserved for future use. This parameter should be set to zero.

### 8.6.8 MTP_USER_PART – MTP User Part

#### Synopsis

The MTP_USER_PART command is used to inform the MTP that a user supplied user part exists on the host.

#### Syntax

```
MTP_USER_PART [<nc_id>] <si> <module_id>
```

#### Example

```
MTP_USER_PART 0x0a 0x2d
MTP_USER_PART NC0 0x0a 0x2d
```

#### Parameters

The MTP_USER_PART command includes the following parameters:

- **<nc_id>**
  SS7 Network Context. The Network Context within which this service indicator to user part association is to apply. Supported values are: NC0, NC1, NC2 or NC3. When the parameter is not present, a value of NC0 is assumed.
- **<si>**
  The service indicator for the user supplied user part in the range 3 to 15.
- **<module_id>**
  The module ID of the user process that receives MTP transfer indications with the specified service indicator value.

### 8.6.9 MONITOR_LINK – Monitor Link

#### Synopsis

The MONITOR_LINK command allows the user to configure a signaling resource (e.g., blink) to monitor signaling operating between two external Switches. The type of interface being listened to is identified by the monitoring type. Received signaling messages are passed directly to a user application without further processing.

***Note:*** Often, applications that use MONITOR_LINK also require the line interfaces to operate in high impedance mode. When using SS7HD boards, high impedance mode can be selected for a particular LIU using the <liu_type> parameter in the LIU_CONFIG command.

#### Syntax

```
MONITOR_LINK <link_id> <if_type> <board_id> <blink> <bpos2> <stream> <timeslot> <user_module> <host id>
<flags>
```

#### Example

```
MONITOR_LINK 0 tdm 1 0-1 1 1 1 0xef 1 0x01
```

#### Parameters

The MONITOR_LINK command includes the following parameters:

- **<link_id>**
  The monitor link's unique logical identity within the SWS. It must be in the range 0 to one less than the maximum number of monitor links supported. The value must not already be allocated to another MONITOR_LINK or MTP_LINK.
- **<if_type>**
  The interface type identifies the type of object being monitored. The monitoring type should be set to one of the following values:

| Mon_type | Description |
|---|---|
| TDM | Single timeslot signaling link |
| E1_HSL | Unstructured E1 HSL.<br>**NOTE:** LIU frame_format must be set to 10. |
| T1_HSL | Unstructured T1 HSL.<br>**NOTE:** LIU frame_format must be set to 10. |
| E1_FRAMED | Framed 31 timeslot E1 HSL |
| T1_FRAMED | Framed 24 timeslot T1 HSL |
| E1_PCM | Structured 30 timeslot E1 HSL (timeslots 0 and 16 are used for signaling) |

  The monitoring type value must be consistent with the liu_type and frame_format values of the LIU_CONFIG command.
- **<bpos>**
  The board identifier of the signaling processor allocated to process the incoming signaling. The board must already have been configured using the SS7_BOARD command..
- **<blink>**
  This is a compound parameter that indicates the signaling processor and the channel on the signaling processor that will be monitored. It is represented in the form **sp_id** - **sp_channel** where:
  - **sp_id** is the identifier of the signaling processor with a value in the range 0 to one less than the number of processors on the board.
  - **sp_channel** is the identifier of the channel on the signaling processor with a value in the range 0 to one less than the number of links supported per signaling processor.

  The MONITOR_LINK and MTP_LINK commands cannot be used on the same sp_id/sp_channel resource. For HSL operation, only one link per signaling processor is supported. Therefore sp_channel must be 0.

- **<bpos2>**
  The board identifier of the stream from which the signaling is to be inserted. The board must have been configured using the SS7_BOARD command. This parameter must be used when setting up link connections across boards. When the SS7_BOARD is configured to be isolated from the internal telephony bus, <bpos2> must equal <bpos>.
- **<stream>**
  When the <timeslot> parameter is set to a non-zero value, the <stream> parameter is the logical identity of the T1/E1 LIU (liu_id) containing the signaling link. It should be in the range 0 to one less than the number of LIUs.
- **<timeslot>**
  The timeslot on the <stream> that should be used for monitoring. For a T1 port, the range is 1 to 24. For an E1 port, the valid range is 1 to 31. The timeslot must not have been previously assigned another MTP or Monitor link.
  For HSL links the timeslot parameter should be set to 0xff to indicate that the link is attached to an LIU configured with the LIU_CONFIG command. HSL might not use timeslots already configured for signaling or data.
- **<user_module>**
  The module ID of the process that will receive the incoming signaling messages, passed as SS7_MSG_RX_IND messages. This should be in the range 0x0d, 0x1d … to 0xfd.
- **<host_id>**
  The logical identifier of the host to which receives SS7_MSG_RX_IND messages.
- **<flags>**
  Per-link flags for monitoring operation. (32 bits)
  - Bit 0 - Set to 1 to enable timestamping of messages monitored by the board for this link. The monitored messages are received in the API_MSG_RX_INDT message type to accomodate the timestamp as well as the received message.
  - Bits 10 and 11 select either 64, 56, or 48 Kbps operation is being monitored, and are used when a link operates over a T1 or E1 timeslot. Use of these bits is as follows:

| Bit 11 | Bit 10 | Rate | Timeslot Usage |
|---|---|---|---|
| 0 | 0 | 64 Kbps | Set both to zero for E1_HSL and T1_HSL operation. HSL framed operation uses these bits in a similar manner to single timeslot signaling to select 64 Kbps, 56 Kbps or 48 Kbps operation that applies to all timeslots within the HSL link. |
| 0 | 1 | 48 Kbps | bits 7&8 not used |
| 1 | 1 | 56 Kbps | bit 8 not used |

  - Bit 12 - sequence number length. Set to 1 the HSL signaling link will use a 12-bit sequence number. Set to 0, the HSL signaling link will use a 7-bit sequence number.

  All other bits should be set to 0.

## 8.7 SIGTRAN Configuration Commands

The SIGTRAN commands include:

- STN_LAS - SIGTRAN Local Application Server Configuration
- STN_LBIND - SIGTRAN Local Bind Configuration
- STN_LINK - SIGTRAN Link Configuration
- STN_NC - SIGTRAN Network Context
- STN_RAS - SIGTRAN Remote Application Server Configuration
- STN_RASLIST - SIGTRAN Remote Application Server List Configuration
- STN_ROUTE - SIGTRAN Route Configuration
- STN_RSGLIST - SIGTRAN Route signaling Gateway List Configuration

### 8.7.1 STN_LAS – SIGTRAN Local Application Server Configuration

#### Synopsis

This command initiates a local application server. An application server is a logical entity representing a SS7 end point.

#### Syntax

```
STN_LAS [<nc_id>] <las> <opc> <rc> <trmd> <flags>
```

#### Examples

```
STN_LAS NC2 1 1200 1 LS 0x0000
STN_LAS     2 1300 2 OR 0x0000
```

#### Parameters

The STN_LAS command has the following parameters:

- **<nc_id>**
  SS7 Network Context. The Network Context together with the Originating Point Code (OPC) uniquely identify an SS7 node by indicating the specific SS7 network it belongs to. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2 or NC3. The parameter is only applicable for M3UA operation.
- **<las >**
  Logical reference for a Local Application Server. The valid range is 0-199.
- **<opc>**
  Specifies an Originating Point Code (OPC) value for the local Application Server.
- **<rc>**
  The logical routing context of the local application server. An RC might not be associated with any other LAS. The valid range is 0: 2147483647.
- **<trmd>**
  The traffic mode for the local application Server. Acceptable values are LS (Loadshare), OR (Override) or BC (Broadcast). Only Loadshare should be used when the SWS is acting as part of a SWS Pair.
- **<flags >**
  This is a 16 bit value used to specify run time options:

| Bit | Description |
|---|---|
| 0 | When set, the configured routing context will be ignored and no routing context will be transmitted. |
| 1-15 | Reserved and should be set to zero. |

#### Prerequisites

In dual mode, only one LAS per NC is permitted.

### 8.7.2 STN_LBIND – SIGTRAN Local Bind Configuration

#### Synopsis

This command associates the local application server with the Remote Application Server or Remote Signaling Gateway, identifying the route to reach the destination.

The software supports M3UA IPSP Single Ended (SE) communication; therefore, the Remote Application Server must have the same routing context as the Local Application Server. When communicating with multiple Remote Application Servers there must be additional Local Application Servers, each having a different routing context.

#### Syntax

```
STN_LBIND <bind> <las> <ras> <flags>
STN_LBIND <bind> <las> <rsg> <flags>
```

#### Example

```
STN_LBIND 1  16  2  0x0000
```

#### Parameters

The STN_LBIND command has the following parameters:

- **<bind >**
  Logical identifier for a binding between a Local Application Server and either a Remote Application Server or Remote Signaling Gateway. The valid range is 0-199.
- **<las >**
  Logical reference for a Local Application Server. An underlying snlink may only be associated with a single LAS. The valid range is 0-199.
- **<ras >**
  Remote Application Server. The Remote Application Server must be associated with at least one SIGTRAN Link and cannot be bound to more than one Local Application Server. In IPSP operation, the Local Application Server and Remote Application Server must be associated with same network context. The valid range is 0-255.
- **<rsg >**
  Remote Signaling Gateway. The Remote Signaling Gateway must be associated with at least one SIGTRAN Link. The valid range is 0-255.
- **<flags >**
  This is a 16 bit value used to specify run time options. This field is reserved for future use and should be set to 0.

### 8.7.3 STN_LINK – SIGTRAN Link Configuration

#### Synopsis

The SIGTRAN link configuration command supports both M2PA and M3UA SIGTRAN links.

#### Syntax

STN_LINK M2PA <snlink> <m2pa_id > <rip1> <rip2> <end>

<lport> <rport> <flags> <lip1> <lip2>

STN_LINK [<nc_id>] M3UA <snlink> <rip1> <rip2> <end>

<lport> <rport> <flags> <rserver> <na> <lip1> <lip2>

Examples

STN_LINK M2PA 4 3 123.12.12.123 0.0.0.0 S

2805 2805 0x0001 123.12.12.124 0.0.0.0

STN_LINK NC1 M3UA 120 123.12.12.123 120.12.12.123 C

3805 3805 0x000e 1 4 123.12.12.124 120.12.12.124

The STN_LINK command has the following parameters:

- <**nc_id**>
  SS7 Network Context. The Network Context the specific SS7 network the SIGTRAN Link is operating with. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2 or NC3. The parameter is only applicable for M3UA operation.
- <**type**>
  Identifies the SIGTRAN protocol and should be set to either M2PA or M3UA.
- <**snlink**>
  Logical reference for a SIGTRAN link; acceptable values are 0-255. A snlink is unique to one link and cannot be re-used by another type.
- <**m2pa_id**>
  A M2PA identifier, in the range 0 to one less than the maximum number of M2PA links supported. Used for M2PA configuration only.
- <**rip1**>
  The primary IP address on which the SWS will attempt to communicate with the remote unit. An rip1 value of 0.0.0.0 cannot be specified.
- <**rip2**>
  The secondary IP address on which the SWS will attempt to communicate with the remote unit. Should be set to 0.0.0.0 if not configured.
- <**end**>
  Identifies whether the SWS end of the SIGTRAN link acts as a CLIENT or a SERVER.
- <**lport**>
  Local (SWS) SCTP port in the range 1 to 65535.
- <**rport**>
  Remote SCTP port in the range 1 to 65535.
- <**flags**>
  This is a 16 bit value used to specify run time options.

| Bit | Description |
|---|---|
| 0 | Secure Mode. When set to 1, the SIGTRAN link will not come into service if it receives a message from an IP address not associated with the SIGTRAN link. |
| 1 | For a M3UA SIGTRAN link communicating with a Remote Signaling Gateway, when set to 1, a DAUD message will be sent when the link comes into service and periodically thereafter. When not set DAUD message will not be generated. Not applicable for M2PA. |
| 2 | For M3UA, set to 1 when the RSG parameter value will be used. Not applicable for M2PA. |
| 3 | For M3UA, set to 1 when the NA parameter value will be used. Not applicable for M2PA. |
| 4-15 | Reserved and should be set to zero. |

- <**rsg**>
  Remote Signaling Gateway (RSG). Identifies a remote server to act as a Remote Signaling Gateway. The RSG might not have the same id value as an existing Remote Application Server. No more than 32 SNLINKs can identify the same RSG. All SIGTRAN links between the SWS and a Remote Signaling Gateway must be of the same protocol type.The valid range is 0-199. Used for M3UA configuration only.
- <**na**>
  The logical network appearance used in communicating with a remote server. The valid range is 0:16777215. Used for M3UA configuration only.

- <**lip1**>
  The first local IP address to be used in the association. lip1 cannot be set to 0 and cannot be the same as lip2 . If a local IP address is configured on one STN_LINK, then each subsequent STN_LINK must have at least one local IP address configured.
- <**lip2**>
  The second local IP address to be used in the association. Should be set to 0 if not configured. It cannot be the same as lip1.

### 8.7.4 STN_NC – SIGTRAN Network Context

#### Synopsis

This command identifies the Network Context and point code size to be used by M3UA.

#### Syntax

```
STN_NC <nc> <ss7mode> <flags>
```

#### Example

```
STN_NC NC3  ITU14  0x0000
```

#### Parameters

The STN_NC command has the following parameters:

- **<nc_id>**
  SS7 Network Context. The Network Context uniquely identifies a SS7 network. Supported values are: NC0, NC1, NC2, or NC3. Only one network context may be configured for M3UA SIGTRAN operation.
- **<ss7mode>**
  The SS7 mode of the network context. Possible values are:

  | | |
  |---|---|
  | **ITU14** | ITU 14 bit operation. |
  | **ITU16** | ITU 16 bit operation. |
  | **ITU24** | ITU 24 bit operation. |
  | **ANSI** | ANSI 24 bit operation. |

- **<flags>**
  This is a 16 bit value used to specify run time options:
  Bit 0 - Enables SLS bit rotation. When set, the SLS field is bit rotated after Signaling Gateway selection and prior to MSU transmission.
  All other bits are reserved for future use.

### 8.7.5 STN_RAS – SIGTRAN Remote Application Server Configuration

#### Synopsis

This command initiates a Remote Application Server.

#### Syntax

```
STN_RAS [<nc_id>] <ras> <dpc> <rc> <nasp> <flags>
```

#### Example

```
STN_RAS  NC2  16  14065  1  2  0x0000
```

#### Parameters

The STN_RAS command has the following parameters:

- **<nc_id>**
  SS7 Network Context. The Network Context together with a Destination Point Code (DPC) uniquely identify an SS7 node by indicating the specific SS7 network it belongs to. When not specified, a value of

NC0 is assumed. Supported values are: NC0, NC1, NC2 or NC3. The parameter is only applicable for M3UA operation.

- **<ras>**
  Remote Application Server, The Remote Application Server might not have the same ID value as an existing Remote Signaling Gateway. The valid range is O-**255.**
- **<dpc>**
  Specifies an Destination Point Code (DPC) value for the Remote Application Server. Only one RAS, SNRT or C7RT can be configured with a particular DPC within a network context.
- **<rc>**
  The logical routing context used in communicating with a remote server. An RC might not be associated with any other remote server. The valid range is 0: 2147483647.
- **<nasp>**
  The number of ASP (SIGTRAN Links) required in load sharing mode.
- **<flags>**
  This is a 16 bit value used to specify run time options:

| Bit | Description |
|---|---|
| 0 | When set, the configured routing context will be ignored and a routing context will not be required from a received remote application server in an activate message |
| 1-15 | Reserved and should be set to zero. |

### 8.7.6 STN_RASLIST – SIGTRAN Remote Application Server List Configuration

#### Synopsis

This command attaches a list of SIGTRAN links to a Remote Application Server. The SIGTRAN links provide the SCTP associations to reach the Remote Application Server.

#### Syntax

```
STN_RASLIST <ras_list> <rserver> <snlink>
```

#### Examples

```
STN_RASLIST 1 16 1
STN_RASLIST 2 16 2
STN_RASLIST 3 16 32
```

#### Parameters

The STN_RASLIST command has the following parameters:

- **<ras_list>**
  Logical identifier for a RAS to SNLINK relationship. The valid range is 0-6399.
- **<ras>**
  Remote Application Server. The valid range is 0-255.
- **<snlink>**
  Logical reference for a SIGTRAN Link. The SIGTRAN link cannot be M2PA and cannot already be attached to this server. A RAS cannot have more than 32 snlinks (4 when loadsharing). A snlink may only be associated with a single Remote Application Server. The valid range is 0-255.

### 8.7.7 STN_ROUTE – SIGTRAN Route Configuration

#### Synopsis

This command is used to configure a SIGTRAN route to a remote SS7 destination.

#### Syntax

```
STN_ROUTE [<nc_id>] <route> <dpc> <flags>
```

### Examples

```
STN_ROUTE NC0  1  100  0x0000
STN_ROUTE      2  200  0x0000
```

### Parameters

The STN_ROUTE command has the following parameters:

- **<nc_id>**
  SS7 Network Context. The Network Context together with the Destination Point Code (DPC) uniquely identify an SS7 node by indicating the specific SS7 network it belongs to. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2 or NC3. The parameter is only applicable for M3UA operation.
- **<route>**
  Logical reference for a SIGTRAN Route. The valid range is 0-255.
- **<dpc>**
  Specifies an Destination Point Code (DPC) value for the Remote Application Server. Only one Remote Application Server, SIGTRAN Route or C7 Route can be configured with a particular DPC within a network context.
- **<flags>**
  This is a 16 bit value used to specify run time options:

| Bit | Description |
|---|---|
| 0 | Route is assumed to be available. |
| 1 | Route will loadshare between all Signaling Gateways in the route. |
| 2-15 | Reserved and should be set to zero. |

## 8.7.8 STN_RSGLIST – SIGTRAN Route signaling Gateway List Configuration

### Synopsis

This command attaches Signaling Gateways to a SIGTRAN Route.

### Syntax

```
STN_RSGLIST <list> <route> <rsg> <flags>
```

### Examples

```
STN_RSGLIST  0  1  1 0x0001
STN_RSGLIST  1  2  1 0x0001
STN_RSGLIST  2  3  1 0x0001
```

### Parameters

The STN_RSGLIST command has the following parameters:

- **<list>**
  Logical identifier for a SIGTRAN Route to Signaling Gateway relationship. The valid range is 0-6399.
- **<route>**
  Logical reference for a SIGTRAN Route. The valid range is 0-255.
- **<rsg>**
  Remote Signaling Gateway. A Signaling gateway can be associated with a route only once. The Signaling Gateway must have at least 1 snlink associated with it. The signaling gateway cannot be attached to more than 255 SIGTRAN routes (4 when loadsharing). A SIGTRAN route cannot have more than 2 signaling gateways associated with it. The valid range is 0-255.
- **<flags>**
  This is a 16 bit value used to specify run time options:
  Bit 0 - When set, the SWS will consider the route via the specified server to be available without waiting for a destination available (DAVA) message.
  All other bits are reserved for future use.

## 8.8 SCCP Configuration Commands

The SCCP configuration commands include:

- SCCP_CONFIG - SCCP Configuration
- SCCP_GTT - Global Title Translation
- SCCP_GTT_ADDRESS - Global Title Translation Address
- SCCP_GTT_PATTERN - Global Title Translation Pattern
- SCCP_SSR - SCCP Network Context Configuration
- SCCP_SSR - SCCP Sub-System Resources
- SCCP_CONC_SSR - SCCP Concerned Sub-Systems Configuration

### 8.8.1 SCCP_CONFIG – SCCP Configuration

#### Synopsis

The SCCP_ CONFIG command defines the global configuration parameters for SCCP when existing in a single network or for Network Context 0 (NC0) when existing in multiple Network Contexts. The SCCP_CONFIG command is used to configure and activate the SCCP and TCAP protocols on the SIU. This command should only be used if the SCCP and TCAP software has been licensed and configured on the SIU.

#### Syntax

```
SCCP_CONFIG <local_spc> <ssf> <options> <auto_uis>
```

#### Example

```
SCCP_CONFIG 123 8 0 1
```

#### Parameters

The SCCP_CONFIG command includes the following parameters:

- **<local_spc>**
  The local point code of the SIU.
- **<ssf>**
  The sub-service field value that SCCP uses when exchanging messages with the MTP. This must always be set so that the Network Indicator bits (the two most significant bits of the 4-bit ssf value) match those set in the MTP_LINKSET command.
- **<options>**
  A 32-bit value containing run-time options for the operation of the SCCP module. The 16 most significant bits provide ext_options, as defined in the *SCCP Programmer's Manual*.
  - Bit 0 should always be set to 0.
  - Bit 1 should always be set to 1.
  - Bit 20 should be set to 1 when using SCCP in conjunction with DTS and dual resilient configuration.
  - The meanings of the remaining bits are as defined for the **options** parameter described in the Configuration Request section of the *SCCP Programmer's Manual*.
- <**auto_uis**>
  Allows the user to disable automatic generation of "user in service" thus allowing applications to indicate when they are in service using a SCP_MSG_SCMG_REQ message. Possible values are:
  - 0: Do not automatically send "user in service" messages; local subsystems must send them.
  - 1: Automatically sends a "user in service" message to SCCP for all configured local subsystems.

  The parameter will default to 1 if not entered.

### 8.8.2 SCCP_NC_CONFIG – SCCP Network Context Configuration

#### Synopsis

The SCCP_NC_CONFIG command defines the global configuration parameters for SCCP existing in an additional SS7 Network Context to that identified by the SCCP_CONFIG command.

#### Syntax

```
SCCP_NC_CONFIG <nc_id> <local_spc> <ssf> <options> <auto_uis>
```

#### Example

```
SCCP_NC_CONFIG  NC1 123 8 0 1
```

#### Parameters

The SCCP_NC_CONFIG command includes the following parameters:

- **<nc_id>**
  SS7 Network Context. This parameter uniquely identifies the SS7 network for which SCCP is being configured. Supported values are: NC1, NC2 and NC3.
- **<local_spc>**
  The local point code of the SIU.
- **<ssf>**
  The sub-service field value that SCCP uses when exchanging messages with the MTP. This must always be set so that the Network Indicator bits (the two most significant bits of the 4-bit ssf value) match those set in the MTP_LINKSET command.
- **<options>**
  A 32-bit value containing run-time options for the operation of the SCCP module. The 16 most significant bits provide ext_options, as defined in the *SCCP Programmer's Manual*.
  - Bit 0 should always be set to 0.
  - Bit 1 should always be set to 1.
  - Bit 20 should be set to 1 when using SCCP in conjunction with DTS and dual resilient configuration.

  The meanings of the remaining bits are as defined for the **options** parameter described in the Configuration Request section of the *SCCP Programmer's Manual*.
- <**auto_uis**>
  Allows the user to disable automatic generation of "user in service" thus allowing applications to indicate when they are in service using a SCP_MSG_SCMG_REQ message. Possible values are:
  - 0: Does not automatically send "user in service" messages; local subsystems must send them.
  - 1: Automatically sends a "user in service" message to SCCP for all configured local subsystems.

  The parameter will default to 1 if not entered.

### 8.8.3 SCCP_GTT – Global Title Translation

#### Synopsis

The SCCP_GTT statement adds a translation to the SCCP global title translation table. This command must be specified after the SCCP_GTT_PATTERN and SCCP_GTT_ADDRESS commands.

> ***Note:*** The pattern, mask, primary and backup addresses referenced by this command must have an identical number of sections.

#### Syntax

```
SCCP_GTT [<nc_id>] <pattern_id> <mask>
<primary_address_id> [<backup_address_id>]
```

#### Example

```
SCCP_GTT 5 R-/K 9
```

**Parameters**

- **<nc_id>**
  SS7 Network Context. The Network Context together with a Signaling Point Code (SPC) uniquely identifies an SS7 node by indicating the specific SS7 network it belongs to. When not specified, a value of NC0 is assumed. Supported values are NC0, NC1, NC2, or NC3.
- **<patt_id>**
  Identifies the pattern specified by the SCCP_GTT_PATTERN command. This value is also used to index the translation within the SCCP module.
- **<mask>**
  This is an expression detailing the operation to be applied to each section of the global title pattern. The format is exactly one operation per section and must contain exactly the same number of sections as the <gtai_pattern> parameter of the associated SCCP_GTT_PATTERN command and the <gtai_replacement> parameter of the associated SCCP_GTT_ADDRESS command.
  The mask can contain the following:

| Mnemonic | Function |
|---|---|
| - | Padding (ignored). |
| / | Separator used to split the mask into sections. |
| K or KEEP | The digits in the corresponding section of the global title address information undergoing translation will be preserved. |
| R or REPLACE | The digits in the corresponding section of the global title address information will be deleted and the digits in the corresponding section of the primary or backup address will be inserted in their place. |

- **<primary_addr_id>**
  Identifies the SCCP_GTT_ADDRESS command the use as the primary translation.
- **<backup_addr_id>**
  Identifies the SCCP_GTT_ADDRESS command the use as the backup translation.

### 8.8.4 SCCP_GTT_ADDRESS – Global Title Translation Address

**Synopsis**

The SCCP_GTT_ADDRESS command defines the global title to be used as the primary or backup destination of a translation. This command must be specified after the SCCP_GTT_PATTERN command. The global title address information of this command is combined with the global title being translated by examining the mask provided in the SCCP_GTT command.

**Syntax**

```
SCCP_GTT_ADDRESS [<nc_id>] <address_id> <addr_indicator>
<pc> <ssn> <global_title> [<gtai_replacement>]
```

**Example**

```
SCCP_GTT_ADDRESS 9 0x11 0x1234 0 0x001104 0-/-
```

**Parameters**

- **<nc_id>**
  SS7 Network Context. The Network Context together with a Signaling Point Code (SPC) uniquely identifies an SS7 node by indicating the specific SS7 network it belongs to. When not specified, a value of NC0 is assumed. Supported values are NC0, NC1, NC2, or NC3.
- **<addr_id>**
  A unique ID identifying the address. Values in the range 0 - 1023 are valid. A maximum of 256 address_id's may be defined within any or each Network Context.
- **<addr_ind>**
  The Address Indicator octet is formatted according to the point-code format specified in the SCCP_CONFIG <options> parameter and indicates which elements of addressing are present in the

called party address pattern being defined. Bit usage for this parameter differs between the ITU (Q.713) and ANSI (T1.112) specifications.

For ITU, the parameter is defined as:

— Bit 8 - Reserved for national use

— Bit 7 - Routing indicator - 0:Route on GT, 1:Route on SSN

— Bits 6-3 - Global title indicator - the value in these bits indicates what data precedes address information in the global title (so in the context of the SCCP_GTT_PATTERN statement, which octets are expected in the <global_title> parameter). Defined values are:

| | |
|---|---|
| 0000 | No Global title. In this case, the <global_title> parameter value should be 0 (zero, base10 - without 0x prefix) |
| 0001 | Global title includes Nature of Address Indicator (NAI) only. The <global_title> parameter (see below) should be a single hexadecimal octet (prefix 0x followed by two hexadecimal digits), the octet value being the NAI. |
| 0010 | Global title includes Translation Type (TT) only. The <global_title> parameter should be a single hexadecimal octet, the octet value being the TT. |
| 0011 | Global title includes TT, Numbering Plan (NP) and Encoding Scheme (ES). The <global_title> parameter should be two hexadecimal octets (prefix 0x followed by four hexadecimal digits) - the TT in the first octet, the NP and ES (four bits each) in the second octet. |
| 0100 | Global title includes TT, NP, ES and NAI. The <global_title> parameter should be three hexadecimal octets (prefix 0x followed by six hexadecimal digits) - the TT in the first octet, the NP and ES (four bits each) in the second octet and the NAI in the third octet. |

Other values are undefined spares or reserved.

— Bit 2 - SSN Indicator. A 1 indicates that SubSystem Number is used in addressing.

— Bit 1 - PC Indicator. A 1 indicates that Point Code is used in addressing.

For ANSI the parameter is defined as:

— Bit 8 - Designated for national use. 0 indicates that the address is international and 1 indicates that the address is national.

— Bit 7 - Routing indicator -
0: Route on GT
1: Route on DPC and SSN

— Bits 6-3 - Global title indicator - the value in these bits indicates what data precedes address information in the global title (so in the context of the SCCP_GTT_PATTERN statement, which octets are expected in the <global_title> parameter). Defined values are:

| | |
|---|---|
| 0000 | No Global title. In this case, the <global_title> parameter value should be 0 (zero, base10 - without 0x prefix) |
| 0001 | Global title includes TT, Numbering Plan (NP) and Encoding Scheme (ES). The <global_title> parameter should be two hexadecimal octets (prefix 0x followed by four hexadecimal digits) - the TT in the first octet, the NP and ES (four bits each) in the second octet. |
| 0010 | Global title includes Translation Type (TT) only. The <global_title> parameter should be a single hexadecimal octet, the octet value being the TT. |

Other values are undefined spares or reserved.

— Bit 2 - PC Indicator. A 1 indicates that Point Code is used in addressing.

— Bit 1 - SSN Indicator. A 1 indicates that SubSystem Number is used in addressing.

- **<pc>**
  The point code. This is ignored if bit 0 of <addr_indicator> is not set.
- **<ssn>**
  The subsystem number. This is ignored if bit 1 of <addr_indicator> is not set.
- **<global_title>**
  The global title, excluding the global title address information, specified as a string of hexadecimal octets starting with 0x except when the <addr_indicator> indicates that no GT is present, when a value of 0 (zero) should be used.

- **<gtai_replacement>**
  The global title address information to translate to, specified as a string of hexadecimal digits (digit 0xe is reserved) in left-to-right order (i.e., the pairs of digits are *not* swapped as would be the case for a BCD string).
  In addition to hexadecimal digits, this string can contain the following characters:

| Character | Function |
|---|---|
| - | Padding (ignored). |
| / | Separator used to split the pattern into sections. Each section can be processed differently, as specified by the <mask> parameter in the SCP_GTT command. |

### 8.8.5 SCCP_GTT_PATTERN – Global Title Translation Pattern

#### Synopsis

The SCCP_GTT_PATTERN command defines the received global title pattern to be matched for a global title translation.

#### Syntax

```
SCCP_GTT_PATTERN [<nc_id>] <pattern_id> <addr_indicator>
<pc> <ssn> <global_title> [<gtai_pattern>]
```

#### Example

```
SCCP_GTT_PATTERN 5 0x10 0x0000 0 0x001104 44/+
```

#### Parameters

- **<nc_id>**
  SS7 Network Context. The Network Context together with a Signaling Point Code (SPC) uniquely identifies an SS7 node by indicating the specific SS7 network it belongs to. When not specified, a value of NC0 is assumed. Supported values are NC0, NC1, NC2 or NC3.
- **<pattern_id>**
  A unique ID identifying the pattern. Values in the range 0 - 1023 are valid. A maximum of 256 pattern_id's may be defined within any or each Network Context.
- **<addr_ind>**
  The Address Indicator octet is formatted according to the point-code format specified in the SCCP_CONFIG <options> parameter and indicates which elements of addressing are present in the called party address pattern being defined. Bit usage for this parameter differs between the ITU (Q.713) and ANSI (T1.112) specifications. For ITU, the parameter is defined as:
  - Bit 8 - Reserved for national use
  - Bit 7 - Routing indicator - 0:Route on GT, 1:Route on SSN
  - Bits 6-3 - Global title indicator - the value in these bits indicates what data precedes address information in the global title (so in the context of the SCCP_GTT_PATTERN statement, which octets are expected in the <global_title> parameter). Defined values are:

| | |
|---|---|
| 0000 | No Global title. In this case, the <global_title> parameter value should be 0 (zero, base10 - without 0x prefix) |
| 0001 | Global title includes Nature of Address Indicator (NAI) only. The <global_title> parameter (see below) should be a single hexadecimal octet (prefix 0x followed by two hexadecimal digits), the octet value being the NAI. |
| 0010 | Global title includes Translation Type (TT) only. The <global_title> parameter should be a single hexadecimal octet, the octet value being the TT. |
| 0011 | Global title includes TT, Numbering Plan (NP) and Encoding Scheme (ES). The <global_title> parameter should be two hexadecimal octets (prefix 0x followed by four hexadecimal digits) - the TT in the first octet, the NP and ES (four bits each) in the second octet. |
| 0100 | Global title includes TT, NP, ES and NAI. The <global_title> parameter should be three hexadecimal octets (prefix 0x followed by six hexadecimal digits) - the TT in the first octet, the NP and ES (four bits each) in the second octet and the NAI in the third octet. |

Other values are undefined spares or reserved.

— Bit 2 - SSN Indicator. A 1 indicates that SubSystem Number is used in addressing.

— Bit 1 - PC Indicator. A 1 indicates that Point Code is used in addressing.

For ANSI the parameter is defined as:

— Bit 8 - Designated for national use. 0 indicates that the address is international and 1 indicates that the address is national.

— Bit 7 - Routing indicator
0: Route on GT
1: Route on DPC and SSN

— Bits 6-3 - Global title indicator - the value in these bits indicates what data precedes address information in the global title (so in the context of the SCCP_GTT_PATTERN statement, which octets are expected in the <global_title> parameter). Defined values are:

| | |
|---|---|
| 0000 | No Global title. In this case, the <global_title> parameter value should be 0 (zero, base10 - without 0x prefix) |
| 0001 | Global title includes TT, Numbering Plan (NP) and Encoding Scheme (ES). The <global_title> parameter should be two hexadecimal octets (prefix 0x followed by four hexadecimal digits) - the TT in the first octet, the NP and ES (four bits each) in the second octet. |
| 0010 | Global title includes Translation Type (TT) only. The <global_title> parameter should be a single hexadecimal octet, the octet value being the TT. |

Other values are undefined spares or reserved.

— Bit 2 - PC Indicator. A 1 indicates that Point Code is used in addressing.

— Bit 1 - SSN Indicator. A 1 indicates that SubSystem Number is used in addressing.

- **<pc>**
The point code. This is ignored if bit 0 of <addr_indicator> is not set.
- **<ssn>**
The subsystem number. This is ignored if bit 1 of <addr_indicator> is not set.
- **<global_title>**
The global title, excluding the global title address information, specified as a string of hexadecimal octets starting with 0x except when the <addr_indicator> (see above) indicates that no GT is present, when a value of 0 (zero) should be used.
- **<gtai_patt>**
The pattern of global title address information to match, specified as a string of hexadecimal digits (digit 0xe is reserved) in left-to-right order (i.e., the pairs of digits are not swapped as would be the case for a BCD string).
As well as hexadecimal digits, this string can contain the following characters:

| Character | Function |
|---|---|
| - | Padding (ignored). |
| + | Wildcard - matches any number of digits |
| ? | Wildcard - matches exactly one digit. |
| / | Separator used to split the pattern into sections. Each section can be processed differently, as specified by the <mask> parameter in the SCP_GTT command. |
| **NOTE:** The "+" wildcard is not "greedy". It matches the shortest possible string of digits, that is, a pattern such as "12+67" matches "1234567", but does not match "1236767". | |

### 8.8.6 SCCP_SSR – SCCP Sub-System Resources

The SCCP_SSR configuration command can be used to configure three types of sub-system resources:

- SCCP remote signaling points (see Section 8.8.6.1)
- SCCP local sub-systems (see Section 8.8.6.2)

- SCCP remote sub-systems (see Section 8.8.6.3)

### 8.8.6.1 Configuring SCCP Remote Signaling Points

#### Synopsis

Each remote signaling point that the SCCP is able to communicate with must be assigned using an SCCP_SSR command. This includes the adjacent signaling point and all remote signaling points.

#### Syntax

```
SCCP_SSR [<nc_id>] <ssr_id> RSP <remote_spc> <rsp_flags> [<pc_mask>]
```

#### Example

```
SCCP_SSR 1 RSP 1236 0
SCCP_SSR NC1 1 RSP 1236 0
```

#### Parameters

The SCCP_SSR command includes the following parameters when configuring SCCP remote signaling points:

- **<nc_id>**
  SS7 Network Context. This parameter uniquely identifies the SS7 network that the SSR is being configured for. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2, or NC3.
- **<ssr_id>**
  A unique value in the range 0 to 2047 that is used to identify the SSR. 512 ssr_ids are allowed per Network Context. The same ssr_id might not be used to configure an SSR of another type.
- **RSP**
  Identifies the SCCP_SSR command type as a command for a remote signaling point.
- **<remote_spc>**
  The point code of the remote signaling point, which may be either an STP or an SCP.
- **<rsp_flags>**
  A 16-bit value, where each bit enables or disables additional features of the remote signaling point. The meaning for each bit is as defined for the options parameter defined in the *Configure Sub-System Resource Request* section of the *SCCP Programmer's Manual*.
- **<pc_mask>**
  A 32-bit value that specifies the part of a destination point code that must match the <remote_spc> value in order for an SCCP transmit message to be sent down to this destination sub-system. Bits set to zero indicate that the corresponding bit position in the transmit message destination point code must match the bit position of the remote SPC. Bits set to 1 indicate bit positions in the message destination point code that do not need to match the remote SPC set for this RSP. This allows configuration of a default destination sub-system (for example, a gateway SCP).

### 8.8.6.2 Configuring SCCP Local Sub-Systems

#### Synopsis

Each local SCCP sub-system is configured using an SCCP_SSR command, specifying the local sub-system number (as used by the SS7 protocol) and the module ID designated by the user to implement this sub-system.

#### Syntax

```
SCCP_SSR [<nc_id>] <ssr_id> LSS <local_ssn> <module_id> <lss_flags> <protocol>
```

#### Example

```
SCCP_SSR 3 LSS 0x07  0x45 1 MAP
SCCP_SSR NC1 3 LSS 0x07  0x45 1 MAP
```

#### Parameters

The SCCP_SSR command includes the following parameters when configuring SCCP local sub-systems:

- **<nc_id>**
  SS7 Network Context. This parameter uniquely identifies the SS7 network that the SSR is being configured for. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2 or NC3.
- **<ssr_id>**
  A unique value in the range 0 to 2047 that is used to identify the SSR. 512 ssr_ids are allowed per Network Context. The same ssr_id might not be used to configure an SSR of another type.
- **LSS**
  Identifies the SCCP_SSR command type as a command for a local SCCP sub-system.
- **<local_ssn>**
  The local sub-system number as defined by the SCCP protocol.
- **<module_id>**
  Set to 0x45 for correct SWS operation.
- **<lss_flags>**
  A 16-bit value where each bit enables or disables additional features of the local sub-system. The meaning of each bit is as defined for the **options** parameter described in the *Configure Sub-System Resource Request* section of the *SCCP Programmer's Manual*.
- **<protocol>**
  Set to MAP.
  For example, to configure a local sub-system (SSN=8) for use in SWS mode the following command would be used:

```
SCCP_SSR 3 LSS 0x08 0x45 0x0000 MAP
```

### 8.8.6.3 Configuring SCCP Remote Sub-Systems

#### Synopsis

This command defines a remote sub-system known to the SIU. Each entry contains the signaling point code and sub-system number. Multiple SCCP_SSR entries may be included in the file. The presence of an RSS command causes the SCCP to generate sub-system test (SST) messages for the sub-system.

#### Syntax

```
SCCP_SSR [<nc_id>] <ssr_id> RSS <remote_spc> <remote_ssn> <rss_flags>
```

#### Example

```
SCCP_SSR 4 RSS 1236 0x67 0
SCCP_SSR NC1 4 RSS 1236 0x67 0
```

#### Parameters

The SCCP_SSR command includes the following parameters when configuring SCCP remote sub-systems:

- **<nc_id>**
  SS7 Network Context. This parameter uniquely identifies the SS7 network that the SSR is being configured for. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2, or NC3.
- **<ssr_id>**
  A unique value in the range 0 to 2047 that is used to identify the SSR. 512 ssr_ids are allowed per Network Context. The same ssr_id might not be used to configure an SSR of another type.
- **RSS**
  Identifies the SCCP_SSR command type as a command for a remote SCCP sub-system.
- **<remote_spc>**
  The point code where the remote sub-system is implemented.

***Note:*** For correct operation, <remote_spc> must always have its own SCCP_RSP entry in addition to any SCCP_RSS entries. There must also be an MTP_ROUTE defined for this signaling point.

- **<remote_ssn>**
  The remote sub-system number as defined by the SCCP protocol.
- **<rss_flags>**
  A 16-bit value where each bit enables or disables additional features of the remote sub-system. The meaning for each bit is as defined for the **options** parameter described in the *Configure Sub-System Resource Request* section of the *SCCP Programmer's Manual*.

### 8.8.7 SCCP_CONC_SSR – SCCP Concerned Sub-Systems Configuration

#### Synopsis

This command defines an SCCP concerned resource that receives SCCP notifications if the state of a resource it is concerned about changes. A concerned sub-system resource, (CSSR), can refer to up to 32 sub-system resources, (SSR).

Notification is given in the form of an SCCP management indication. Multiple SCCP_CONC_SSR entries may be included in the file. See the *SCCP Programmer's Manual* for more information.

#### Syntax

```
SCCP_CONC_SSR [<nc_id>] <id> <cssr_id> <ssr_id>
```

#### Example

```
SCCP_CONC_SSR 1 4 2
SCCP_CONC_SSR NC1 1 4 2
```

#### Parameters

The SCCP_CONC_SRR command includes the following parameters:

- **<nc_id>**
  SS7 Network Context. This parameter uniquely identifies the SS7 network that the SSR is being configured for. When not specified, a value of NC0 is assumed. Supported values are: NC0, NC1, NC2 or NC3.
- **<id>**
  A unique value in the range 0 to 8191 that is used to identify the concerned sub-system resource command.
- **<cssr_id>**
  Refers to a concerned resource specified by an SCCP_SSR command. The <cssr_id> may identify SSRs of two types: LSS and RSP. The <cssr_id> identifies the concerned resource that receives SCCP notifications if the state of the controlled resource identified by the <ssr_id> is changed.
- **<ssr_id>**
  Refers to a controlled resource specified by an SCCP_SSR command:
  - If the <cssr_id> is referring to an LSS, the <ssr_id> used in the same command may refer to either an RSS or an RSP resource.
  - If the <cssr_id> is referring to an RSP, the <ssr_id> used in the same command can only refer to an LSS resource.

***Note:*** The <cssr_id> and <ssr_id> parameters can only refer to SSR's previously configured using the SCCP_SSR command.

## 8.9 TCAP Configuration Commands

The TCAP configuration commands include:

- TCAP_CONFIG - TCAP Configuration
- TCAP_NC_CONFIG - TCAP Network Context Configuration
- TCAP_CFG_DGRP - TCAP Dialog Group Configuration

### 8.9.1 TCAP_CONFIG – TCAP Configuration

#### Synopsis

The TCAP_CONFIG command activates the TCAP protocol layer on the SWS and provides the TCAP operating parameters. This command should only be used when an SCCP_CONFIG command is present.

***Note:*** Network Context-specific configuration may be done using the TCAP_NC_CONFIG command.

#### Syntax

```
TCAP_CONFIG <base_ogdlg_id> <nog_dialogues> <base_icdlg_id> <nic_dialogues> <options> <dlg_hunt> <addr format>
```

#### Examples

```
TCAP_CONFIG 0x0000 8192 0x8000 8192 0x0000 0 0
```

#### Parameters

The TCAP_CONFIG command includes the following parameters:

- **<base_ogdlg_id>**
  The dialogue_id for the first outgoing dialog.
- **<nog_dialogues>**
  The number of outgoing dialogs to support. The valid range is 0 to 32767.
- **<base_icdlg_id>**
  The dialogue_id for the first incoming dialog. The most significant bit (bit 15) of the dialog ID must be set to one for incoming dialogs.
- **<nic_dialogues>**
  The number of incoming dialogs to support. The valid range is 0 to 32767.

  ***Note:*** If dialogue values are out of the permitted range TCAP will be configured with default values of 32767 nog_dialogues and 32767 nic_dialogues.
- **<options>**
  Specifies TCAP protocol options as defined for the TCAP Configuration Request message in the *TCAP Programmer's Manual*.
- **<dlg_hunt>**
  The hunt mode used in the case of multiple TCAP hosts to determine which TCAP group is selected whenever a new incoming dialog arrives. It should be set to 0, 1 or 2 for the following hunt modes:
  - 0: Cyclic Selection. Each new incoming dialog is allocated to the next TCAP group.
  - 1: Load Balanced Selection. Each new incoming dialog is allocated to the group with the least number of active incoming dialogs.
  - 2: Sequential Selection. Each new incoming dialog is allocated to the group containing the first inactive incoming <dialogue_id>.

- **<addr format>**
  The format of messages used by TCAP. Possible values are:
  - 0: The address format is determined by the setting of bit 1 of the **<options>** field.
    - If bit 1 of the **<options>** field is set to indicate ANSI TCAP PDU formats, then ANSI format 24-bit point codes are selected.
    - If bit 1 of the **<options>** field is not set, ITU-T TCAP PDU formats and 14-bit point codes are selected.
  - 1: ITU-T format, 14-bit point codes
  - 2: ITU-T format, 24-bit point codes
  - 3: ANSI format, 14-bit point codes
  - 4: ANSI format, 24-bit point codes

  ***Note:*** 16-bit point codes are not supported.

### 8.9.2 TCAP_NC_CONFIG – TCAP Network Context Configuration

#### Synopsis

The TCAP_NC_CONFIG command specifies Network Context-specific configuration for TCAP and overrides configuration specified by the TCAP_CONFIG command. This command should only be used when a TCAP_CONFIG command is present.

#### Syntax

```
TCAP_NC_CONFIG <nc_id> <options> <addr format>
```

#### Examples

```
TCAP_NC_CONFIG NC0 0x0000 0
```

#### Parameters

The TCAP_NC_CONFIG command includes the following parameters:

- **<nc_id>**
  SS7 Network Context. This parameter uniquely identifies the SS7 network that TCAP is being configured for. Supported values are: NC1, NC2 or NC3.
- **<options>**
  Specifies TCAP protocol options as defined for the TCAP Configuration Request message in the *TCAP Programmer's Manual*.
- **<addr format>**
  The format of messages used by TCAP. Possible values are:
  - 0: The address format is determined by the setting of bit 1 of the **<options>** field.
    - If bit 1 of the **<options>** field is set to indicate ANSI TCAP PDU formats, then ANSI format 24-bit point codes are selected.
    - If bit 1 of the **<options>** field is not set, ITU-T TCAP PDU formats and 14-bit point codes are selected.
  - 1: ITU-T format, 14-bit point codes
  - 2: ITU-T format, 24-bit point codes
  - 3: ANSI format, 14-bit point codes
  - 4: ANSI format, 24-bit point codes

  ***Note:*** 16-bit point codes are not supported.

### 8.9.3 TCAP_CFG_DGRP – TCAP Dialog Group Configuration

#### Synopsis

The TCAP_CFG_DGRP command allows you to configure TCAP dialog groups, each group handling a sub-set of the total available dialogs. This allows each group to reside on a separate host computer that in turn allows the application using TCAP to be distributed over several machines. If the TCAP_CFG_DGRP command is omitted, the complete range of dialog identifiers defined by the TCAP_CONFIG command is assigned to host_id 0.

#### Syntax

```
TCAP_CFG_DGRP <gid> <base_ogdlg_id> <nog_dialogues> <base_icdlg_id> <nic_dialogues> <options> <host_id>
```

#### Examples

```
TCAP_CFG_DGRP 0 0x0000 1024 0x8000 1024 0 0
TCAP_CFG_DGRP 1 0x0400 1024 0x8400 1024 0 1
```

#### Parameters

The TCAP_CFG_DGRP command includes the following parameters:

- **<gid>**
  A logical identifier for this group, the valid range being 0 to 31.
- **<base_ogdlg_id>**
  The first outgoing dialog ID assigned to this dialog group.
- **<nog_dialogues>**
  The number of outgoing dialogs assigned to this group, hence outgoing dialog IDs base_ogdlg_id to base_ogdlg_id + nog_dialogues-1 are assigned to this group.
- **<base_icdlg_id>**
  The first incoming dialog ID assigned to this dialog identifier group.
- **<nic_dialogues>**
  The number of incoming dialogs assigned to this group, hence outgoing dialog IDs base_ogdlg_id to base_icdlg_id + nic_dialogues-1 are assigned to this group.
- **<options>**
  Should be set to zero.
- **<host_id>**
  Identifies the host computer to which the defined ranges of dialogs will be sent.
  The number of dialogs must lie within the limit specified with the TCAP_CONFIG command.

## 8.10 MAP Configuration Commands

The MAP configuration commands include:

- MAP_CONFIG - MAP Configuration
- MAP_NC_CONFIG - MAP Configuration

### 8.10.1 MAP_CONFIG – MAP Configuration

#### Synopsis

The MAP_CONFIG command defines the global configuration parameters for MAP when existing in a single network or for Network Context 0 (NC0) when existing in multiple Network Contexts. This command should only be used if the MAP software has been licensed and configured on the SIU and must appear on a separate command line in the config.txt file after the SCCP_SSR command that identifies MAP as the protocol module.

#### Syntax

```
MAP_CONFIG <options>
```

### Example

```
MAP_CONFIG 2
```

### Parameters

The MAP_CONFIG command includes the following parameter:

- **<options>**
  A 32-bit value containing run-time options for passing to the MAP module. Individual bit definitions are as specified for the options field in the MAP_MSG_CONFIG command as defined in the *MAP Programmer's Manual*. Currently, this includes two bits as follows:

| Bit | Mnemonic | Description |
|---|---|---|
| 0 | MAPF_V2_ERRORS | V3 dialogs use the V2 error format |
| 1 | MAPF_NO_PREARRANGED_END | Dialogs are closed immediately on reception of CLOSE_REQ |

## 8.10.2 MAP_NC_CONFIG – MAP Configuration

### Synopsis

The MAP_NC_CONFIG command defines the global configuration parameters for MAP existing in an additional SS7 Network Context to that identified by the MAP_CONFIG command.

### Syntax

```
MAP_NC_CONFIG <nc_id> <options>
```

### Example

```
MAP_NC_CONFIG NC1 2
```

### Parameters

The MAP_NC_CONFIG command includes the following parameter:

- **<nc_id>**
  SS7 Network Context. This parameter uniquely identifies the SS7 network that MAP is being configured for. Supported values are: NC1, NC2 or NC3.
- **<options>**
  A 32-bit value containing run-time options for passing to the MAP module. Individual bit definitions are as specified for the options field in the MAP_MSG_CONFIG command as defined in the *MAP Programmer's Manual*. Currently, this includes two bits as follows:

| Bit | Mnemonic | Description |
|---|---|---|
| 0 | MAPF_V2_ERRORS | V3 dialogs use the V2 error format |
| 1 | MAPF_NO_PREARRANGED_END | Dialogs are closed immediately on reception of CLOSE_REQ |

## 8.11 Protocol Configuration Modification

The protocol configuration is specified in an ASCII text file. The commands stored in this file may be modified by transferring the configuration file from a remote machine using FTP. This allows the native editor of the remote computer to be used to modify the configuration file.

A local back-up of the current configuration may be made by entering the CNBUI command at the management terminal. This may be restored after a protocol file edit using the CNBUS command (this overwrites the existing configuration with the last back-up configuration).

The protocol configuration may be returned to the original default configuration by using the CNRDI command.

### 8.11.1 Establishing an FTP Session

An FTP session should be established between the remote machine and the SWS by entering the appropriate command on the remote machine's keyboard, for example:

```
ftp 123.124.125.125
```

The appropriate user name and password to use depend on whether a password has been configured for the siuftp account using the CNUAS MML command.

If a password is configured, then FTP access must use the fixed user name "siuftp" in conjunction with the normal MML access password as configured by setting the CNUAS parameter PASSWORD for the siuftp account. If no password has been configured, then access is gained using a default password 'siuftp'. Access to the SWS using other user accounts except "siuftp" is denied.

The state of FTP password may be viewed using the CNUAP command.

FTP access may be established over SSH using secure FTP. FTP access using secure FTP is similar to normal FTP with the exception that Secure FTP users will by default land in the parent directory of siuftp and will need to change to the siuftp directory before commencing operation. Most Secure FTP clients provide an option to configure the default initial directory. If available, users may choose to use this instead of manually changing to the siuftp subdirectory.

### 8.11.2 Transferring the Protocol Configuration to a Remote Computer

The configuration file may be read from the SWS to a remote computer. The file may then be modified by a native editor running on that computer. Once the modifications are complete, the file may be transferred back to the SWS using FTP.

> ***Note:*** For correct operation, before the configuration file is transferred, the transfer type must be set to text. Most FTP implementations use the **ASCII** command to set text transfer type.

The configuration file config.txt may be transferred to the remote system using the FTP get command:

```
get config.txt
```

The FTP session should then be terminated by entering the **quit** or **bye** command.

Once the protocol configuration file has been modified, this should be transferred back to the SWS using the FTP put command:

```
put config.txt config.txt
```

The SWS uses a case-sensitive file-system. Therefore, it is necessary to specify the name of the target file (the second filename in the example command shown above) in lowercase.

# Chapter 9: Configuration Guidelines

## 9.1 Overview

Configuration guidelines are provided for the following:

- IP Port Bonding
- Configuring a Dual Resilient SWS System
- Configuring an ANSI System
- Specifying Default Routes
- Dynamic Host Activation
- Dynamic Configuration
- SIGTRAN M2PA Signaling
- SIGTRAN M3UA Signaling
- SIGTRAN M3UA - Dual Operation
- GTT Configuration
- HSL Signaling
- ATM Signaling

## 9.2 IP Port Bonding

The SIU allows you to configure a resilient IP connection across an IP port bonding team of two ports in an active/standby configuration. On the Dialogic® DSI SS7G22 and SS7G31 Signaling Servers, up to two port bonding teams may be created using the four Ethernet ports on the SWS. The Dialogic® DSI SS7G32 Signaling Server has 6 Ethernet ports, allowing up to three port bonding teams. Each team has a single IP address configured with a primary (active) and secondary (standby) port. Any IP port on the system may be the primary port in a team and any port may be the secondary port. The primary port is a port configured with the IP address of the team and the secondary port is a port configured with a string to associate it with the primary port (see Section 6.10.1, “IPEPS” on page 83).

If the system detects that the Primary port has failed, it passes the primary's MAC and Layer 3 address to the failover (secondary) adapter, enabling it to act as the active port in the team. On the restoration of the primary port, the secondary port is removed from service and the primary port resumes control of its MAC and IP addresses.

The subnet mask of a secondary IP address in a team is ignored.

Data loss may occur between the actual failure of an IP connect and the detection of that failure and subsequent switching to the standby port.

All adapters in a team should be connected to the same hub or switch with Spanning Tree (STP) set to **off**.

Whenever bonding is activated, or deactivated, MMI sessions using those ports are reset.

An IP address might not be bonded with:

- itself
- an IP address of 0.0.0.0
- another IP address already acting as a primary or standby in an IP team

Once configured, the status of Ethernet ports in a bonded team may be checked using the STEPP command (see Section 6.15.6 on page 105).

## 9.3 Configuring a Dual Resilient SWS System

For the dual resilient configuration, it is necessary to modify the configuration to assign one unit as SWSA and the other as SWSB using the management terminal CNSYS command. Each unit is assigned a unique IP address.

To assign a unit as SWSB, the following command should be used:

```
CNSYS:MODE=SWSB;
```

To assign a unit as SWSA, the following command should be used:

```
CNSYS:MODE=SWSA;
```

***Note:*** The modified configuration is applied only when the unit is restarted.

The inter-SWS link set should be defined on both units using the MTP_LINKSET command with bit 15 of the <**flags**> parameter set to 1. This link set must have the same value defined for the <**local_spc**> and <**adjacent_spc**> values; this is the local point code of the SWS pair. Links are added to the Inter-SWS link set using the MTP_LINK command, assigning incrementing <**link_ref**> and <**slc**> values as used normally. The <**bpos**> and <**blink**> parameters should be set accordingly.

A route should be defined on each unit for the inter-SWS link set using the MTP_ROUTE command referencing the appropriate <**linkset_id**> with a <**dpc**> value set to the point code of the SWS pair.

The management entity within each SWS indicates the availability of the inter-SWS links to the application running on the first host using the message based Application Programming Interface (API).

Additional information for the protocol configuration commands and parameters may be found in the previous sections.

## 9.4 Configuring an ANSI System

This section provides additional guidelines for configuring an SWS to operate in accordance with the ANSI T1 specifications.

The default protocol configuration for an SWS specifies ITU-T protocol behavior. To operate in accordance with ANSI it is necessary to modify the options settings for MTP3 and the User Part held in the protocol configuration file on the SWS.

The MTP_CONFIG <**options**> parameter must have bits 8 to 11 set to 1 (value 0x0f00) to define ANSI operation.

The MTP_LINKSET <**ssf**> parameter must have the least two significant bits (B and A) both set to 1 so that all MTP3 originated messages are assigned a message priority of 3. The two most significant bits (D and C) are the network indicator. Hence valid ANSI ssf values are 0x3, 0x7, 0xb and 0xf.

ANSI operation for the protocol layers above MTP3 is specified using the configuration values specified in the Configuration Section of the appropriate programmer's manual.

The **<ts_mask>** parameter in the example cross connect command applies to an E1 (32-timeslot) PCM connection. This should be modified to reference 24 timeslots for a T1 configuration. Hence, to apply a cross connect to timeslots 1 to 23, (leaving timeslot 24 for SS7) the mask should be set to 0x1fffffe.

Additional information for the protocol configuration commands and parameters may be found in the previous sections.

## 9.5 Specifying Default Routes

For telephony operation, the SWS requires an MTP_ROUTE definition for each signaling point that the local point code(s) communicate with. In addition, transaction-based systems require a declaration of each remote sub-system with an SCCP_SSR command.

It is also possible to configure MTP routes that are designated as "default" routes. Default routes can be used to convey traffic for multiple destinations without the need to configure each Destination Point Code (DPC) as an explicit MTP route. Typically, this is useful when a signaling point connects simply to a single STP or a mated pair of STPs and all traffic can be sent to the STP, irrespective of current network status.

Two types of default route are supported:

- One associated with a “real” DPC. In this case the (default) route is deemed to be accessible whenever the specified DPC is accessible.
- One associated with a “pseudo” DPC, which is a point code that does not exist within the network (for example, zero). In this case the (default) route is deemed to be accessible as soon as the link sets within the route are available.

A maximum of one default route for each supported Service Indicator (or user part) is permitted. Configuration of default routes utilizes bits 2, 3, and 5 in the **<flags>** field of the MTP_ROUTE command.

For transaction based applications, it is also necessary to supply a **<pc_mask>** value with the definition of each SCCP_SSR. The **<pc_mask>** is used to determine which bits of the target point code (the destination point code in the MTP label of the transmit message) should be ignored when selecting the route. The **<pc_mask>** makes it possible to configure a route to a specific destination that is also used for other destinations with a similar point code. This allows configuration of default destination sub-systems (for example, to a gateway SCP).

## 9.6 Dynamic Host Activation

The SWS has the ability to activate/deactivate host links using the MNINI/MNINE commands. This functionality supports the preservation of the host status over a restart and no alarms are reported for those hosts that have been deactivated.

If the SIU_HOSTS configuration command is omitted from the configuration file, all host links are configured, but only the first is activated (the others remain deactivated initially). If the SIU_HOSTS configuration command is present and **<num_hosts>** is specified, then that number of hosts are configured and activated; in this case, no additional hosts can be configured.

This allows the SWS users to escalate their systems by adding or removing host connections at runtime and without the need to apply a system restart to the unit. In the case that a unit restart is required, the configuration adopted can be preserved.

## 9.7 Dynamic Configuration

Dynamic configuration allows you to add, delete, or modify configuration elements (for example, circuit groups) without affecting the state of any other configuration element in the system. Dynamic configuration does not require a system restart. There are two forms of dynamic configuration:

- Config.txt-based dynamic configuration, where the user transmits an updated config.txt file to the system, then executes an MMI command to load the configuration into system memory for use. Since the new configuration exists within a config.txt file, the updated configuration is preserved over a restart. See Section 9.7.1, “Config.txt-Based Dynamic Configuration” on page 173 for more information.
- Application-based dynamic configuration, where a user application transmits a configuration message directly to the protocol module. Since the new configuration does not exist in a config.txt file, the updated configuration is not preserved over a restart and it is therefore necessary for the user application to detect any restart of the SWS and reconfigure the unit as needed.

### 9.7.1 Config.txt-Based Dynamic Configuration

In config.txt-based dynamic configuration, the user transmits an updated config.txt file to the system, then executes an MMI command to load the configuration into system memory for use. Since the new configuration exists within a config.txt file, the updated configuration is preserved over a restart.

The process for config.txt-based dynamic configuration is as follows:

1. Add, delete, or modify the configuration element in the config.txt file.
2. Transfer the config.txt file to the unit via FTP.
3. Invoke the CNURx MMI command to update the unit configuration.

In every case when the SWS is restarted, the configuration file last transferred will be applied to the unit.

The CNURx commands return the following responses:

- RANGE ERROR - the identifier value is invalid

- UNACCEPTABLE COMMAND - the command does not satisfy all prerequisite conditions
- GENERAL ERROR - the config.txt command line is incorrectly formatted or the operation failed to complete successfully – the configuration of the system is restored to the state prior to command execution.

Note the following:

- When adding configuration elements, the elements might not already be configured within the SWS.
- When changing or deleting configuration elements, the elements must already have been previously configured within the SWS.
- When using dynamic configuration all command line parameters, including the element identifier value, are mandatory. Dynamic configuration may fail if the format of the command line does not include all the parameters identified in this manual.

The configuration actions supported for dynamic configuration are described in Table 5.

**Table 5. Supported Actions for Dynamic Configuration**

| Configuration Action | Affected Config.txt Command | CNURI ID | CNURI MODE | Notes |
|---|---|---|---|---|
| MTP Route Addition | MTP_ROUTE | Route ID | MTPR | Current MTP Route configuration may be view using the CNCRP MMI command. |
| SCCP Sub-System Resource addition | SCCP_SSR | SSR ID | SSR | Current SSR configuration may be view using the CNSSP MMI command. |
| SCCP Concerned Sub-System addition | SCCP_CONC_SSR | CSSR ID | CSSR | Current CSSR configuration may be view using the CNCSP MMI command. |
| SIGTRAN Route Addition | STN_ROUTE | SIGTRAN Route ID | M3UAR | Current SIGTRAN route configuration can be identified using the CNSRP command |
| SIGTRAN Route List Addition | STN_RSGLIST | SIGTRAN Rsglist ID | M3UARLIST | Current SIGTRAN route list configuration can be identified using the CNGLP command |
| PCM Addition | LIU_CONFIG | Port ID | LIU | Current PCM configuration may be viewed using the CNPCP MMI command. |
| PCM Deletion | LIU_CONFIG | Port ID | LIU | Current PCM configuration may be viewed using the CNPCP MMI command. |
| MTP Linkset Addition | MTP_LINKSET | Linkset ID | MTPLS | Current Linkset configuration may be viewed using the CNLSP MMI command. |
| MTP Linkset Change | MTP_LINKSET | Linkset ID | MTPLS | The <num links> parameter may be changed on a MTP linkset.<br>Current Linkset configuration may be viewed using the CNLSP MMI command. |
| MTP Linkset Deletion | MTP_LINKSET | Linkset ID | MTPLS | Current Linkset configuration may be viewed using the CNLSP MMI command. |
| MTP Route Change | MTP_ROUTE | Route ID | MTPR | The flags field and the first and second linksrts may be changed on the MTP route command.<br>Current MTP Route configuration may be viewed using the CNCRP MMI command. |
| MTP Route Deletion | MTP_ROUTE | Route ID | MTPR | Current MTP Route configuration may be viewed using the CNCRP MMI command. |

**Table 5. Supported Actions for Dynamic Configuration (Continued)**

| Configuration Action | Affected Config.txt Command | CNURI ID | CNURI MODE | Notes |
|---|---|---|---|---|
| MTP SS7 Link Addition | MTP_LINK | Link ID | MTPL | Links added to SPCI4 Signaling Boards require a board reset and link activation before they can be used.<br>Current MTP SS7 Link configuration may be viewed using the CNSLP MMI command. |
| MTP SS7 Link Deletion | MTP_LINK | Link ID | MTPL | Links removed from SPCI4 Signaling Boards require a board reset to complete their removal. Current MTP SS7 Link configuration may be viewed using the CNSLP MMI command. |
| Monitoring Link Addition | MONITOR_LINK | Link ID | MONL | Current Monitor Link configuration may be viewed using the CNMLP MMI command. |
| Monitoring Link Removal | MONITOR_LINK | Link ID | MONL | Current Monitor Link configuration may be viewed using the CNMLP MMI command. |

## 9.8 SIGTRAN M2PA Signaling

### 9.8.1 Overview

The SWS supports the SIGTRAN M2PA protocol compatible with IETF RFC 4165. M2PA peer- to-peer operation can be employed as the network transport layer, providing services normally provided by MTP2 for SS7 signaling links.

SS7 signaling traffic can be conveyed over SIGTRAN network-facing links to a signaling gateway or other signaling point employing M2PA. In dual configuration, an M2PA link can be used as the SWS-interlink to carry SS7 data between the two units.

Using the STN_LINK command, you can configure up to 256 M2PA links. The STN_LINK command should appear before the MTP_CONFIG command in the config.txt file. Having configured an M2PA link, you can associate this with an SS7 link using the MTP_LINK command.

### 9.8.2 M2PA License

Before M2PA network facing links can be configured, the unit must be equipped with an M2PA license, as listed in Section 4.1.2, “Temporary Licenses” on page 32.

The M2PA license is not required for configuration of M2PA interlinks employed in SWS dual configuration. With the license installed, the CNSYP command will display the M2PA parameter set to Y. Without a license the CNSYP command will not display the M2PA parameter.

### 9.8.3 SS7 over M2PA

An SS7 link is associated with the M2PA link using the MTP_LINK command. SS7 MSUs will then be carried over SIGTRAN as opposed to MTP2.

An SS7 link can only be associated with one M2PA link, and two SS7 links cannot be associated with the same M2PA link. The following commands demonstrate M2PA and SS7 link configuration.

```
STN_LINK M2PA 1 0 123.123.123.1 0.0.0.0 C 2905 2905 0x0000
MTP_LINK 1 2 1 1 0 1 0 0 0x80000006
```

The SS7 link is associated with an M2PA link when bit 31 of the MTP_LINK <flags> parameter is set to 1. The <blink> parameter identifies the M2PA link (link_id). The <bpos> <stream> and <timeslot> parameters should all be set to zero.

### 9.8.4 Configuration Examples

Example configuration of SS7 links conveyed over M2PA.

```
SIU_HOSTS 1
*
*
*   M2PA_CONFIG
*
*         <type ><link_id> <m2pa_id> <ip1>          <ip2>     <end> <hport> <pport> <flags>
*
STN_LINK   M2PA     0         0      172.28.148.96  0.0.0.0    c     2805    2805     0x0000
STN_LINK   M2PA     2         1      172.28.148.96  0.0.0.0    c     3565    3565     0x0000
STN_LINK   M2PA     199       2      172.28.148.96  0.0.0.0    c     3566    3566     0x0000
*
*
*   MTP_CONFIG 0 0 <options>
*
MTP_CONFIG     0 0 0x00000000
*
*
*   MTP_LINKSET <NC> <linkset_id> <adjacent_spc> <num_links> <flags> <local_spc> <ssf>
*
*
MTP_LINKSET      NC0       0              1           16     0x0000      2      0x08
*
*
*
*   MTP_LINK <link_id><linkset_id><link_ref><slc><bpos><blink><stream><timeslot><flags>
*
MTP_LINK         0         0          0       0    0      0      0        0     0x80000006
MTP_LINK         1         0          1       1    0      2      0        0     0x80000006
MTP_LINK         2         0          2       2    0      199    0        0     0x80000006
*
*   MTP_ROUTE <NC>  <dpc><linkset_id><user_part_mask><flags><2nd_ls><pc_mask>
*
*
MTP_ROUTE       NC0   1       0          0x0020       0x0000    0
*
*
* End of file
*
```

## 9.9 SIGTRAN M3UA Signaling

### 9.9.1 Overview

This SWS supports the SIGTRAN M3UA protocol compatible with IETF RFC 3332/4666. M3UA can be deployed as a direct replacement for MTP3 on the SWS with M3UA over SCTP offering a SS7 over IP solution removing the need to deploy TDM SS7 links.

Using M3UA, the SWS can connect either directly to multiple Signaling End Points (SEPs) in a IPSP (peer to peer) configuration, or indirectly via a SIGTRAN Signaling Gateway. M3UA supports load-sharing across a pair of SWSs, configured as a single point code, without the requirement for a TDM SWS interlink between the two units.

M3UA must be configured to operate in a particular network context using the STN_NC command. M3UA may only be active in one network context at a time. MTP and M3UA might not be configured to be in the same network context. A SWS can support both M3UA and MTP operation in different networks contexts, allowing the host application to act as a gateway between TDM based SS7 and SIGTRAN networks.

When a SWS is using M3UA, it is considered be acting as one or more Local Application Servers. Using the STN_LINK command, you can configure up to 256 M3UA links. These links may be connected to either a SIGTRAN Signaling Gateway using the STN_LINK command, or up to 256 Remote Application Servers (Signaling End Points) using the STN_RAS and STN_RASLIST commands. When interworking to a SIGTRAN Signaling Gateway, the SWS can be configured to route to up to 256 Remote Point Codes in the network, using the Signaling Gateway with the STN_ROUTE and STN_RSGLIST commands. Finally, the Local Application Server can be associated with either a Remote Application Server or Signaling Gateway, using the STN_LBIND command.

### 9.9.2 Configuration Examples

#### 9.9.2.1 SWS to Signaling Gateway

Example configuration of an SWS acting as Point Code 3 communicating to point code 2 via a Signaling Gateway.

```
* AS-SG 2 M3UA LINKS.
*
*         <host>
SIU_HOSTS 1
*
*       <nc> <ss7md> <flags>
STN_NC  NC0  ITU14   0x0000
*
*
*       <nc> <type> <link><ip1>          <ip2>   <end>
*        |   |      |     |               |       | <hport>
*        |   |      |     |               |       | |    <pport>
*        |   |      |     |               |       | |    |    <flags>
*        |   |      |     |               |       | |    |    |      <rserver>
*        |   |      |     |               |       | |    |    |      | <na>
*
STN_LINK NC0 M3UA   1     192.219.17.200 0.0.0.0 C 2905 2905 0x0006 1 0
STN_LINK NC0 M3UA   2     192.219.17.200 0.0.0.0 C 2906 2906 0x0006 1 0
*
*
*         <NC> <LAS> <OPC> <RC> <TRMD> <flags>
STN_LAS    NC0  1     3    1     LS    0x0000
*
*         <NC>  <ROUTE>  <DPC>  <flags>
STN_ROUTE  NC0  1        2      0x0000
*
*          <list> <route> <rserver>  <flags>
STN_RSGLIST  1         1      1       0x0000
*
*
*         <BIND> <LAS> <RSERVER> <FLAGS>
STN_LBIND 1      1     1         0x0000
*
* User part configuration e.g. SCCP.
```

#### 9.9.2.2 SWS to Remote Application Server (IPSP Operation)

Example configuration of an SWS in IPSP operation using 4 links to connect with 2 remote application servers.

```
* M3UA config to connect SWS to 2 RAS (IPSP)using 4 LINKS
*         <host>
SIU_HOSTS   1
*
*       <nc> <ss7md> <flags>
STN_NC  NC0  ITU14   0x0000
*
*       <nc> <type> <link> <ip1>      <ip2>   <end>
*        |   |      |      |          |       | <hport>
*        |   |      |      |          |       | |    <pport>
*        |   |      |      |          |       | |    |    <flags>
*        |   |      |      |          |       | |    |    |      <rserver>
*        |   |      |      |          |       | |    |    |      | <na>
STN_LINK NC0 M3UA   0       123.1.2.3  0.0.0.0 C 2905 2905 0x0000 0 0
STN_LINK NC0 M3UA   1       123.1.2.3  0.0.0.0 C 2906 2906 0x0000 0 0
STN_LINK NC0 M3UA   2       123.1.2.3  0.0.0.0 C 2907 2907 0x0000 0 0
STN_LINK NC0 M3UA   3       123.1.2.3  0.0.0.0 C 2908 2908 0x0000 0 0

*
*         <nc>  <id>  <opc>  <rc>  <trmd>  <flags>
STN_LAS          0     100    1      LS     0x0000
STN_LAS          1     100    2      LS     0x0000

*
*         <nc>  <rserver>  <dpc>  <rc>  <nasp>  <flags>
STN_RAS          0          10     1      1      0x0000
```

```
STN_RAS          1          11     2      1      0x0000

*
*
*           <list> <rserver> <link>
STN_RASLIST   0        0       0
STN_RASLIST   0        0       1
STN_RASLIST   1        1       2
STN_RASLIST   1        1       3

*
*
*          <bind>  <las>  <rserver>  <flags>
STN_LBIND    0       0       0        0x0000
STN_LBIND    1       1       1        0x0000

*
* User part configuration e.g. SCCP.
```

## 9.10 SIGTRAN M3UA - Dual Operation

M3UA on a pair of SWSs can offer a level of resilience similar to that supported by a pair of SWSs operating MTP3. When configured, the SWSs will each behave as an Application Server Process operating within an Application Server; thus presenting a single point code to the network.

In the same manner as MTP3 resilient operation, one SWS should be configured as SWSA and the other as SWSB using the CNSYS command. Also in the same manner as MTP3, the configuration command SIU_REM_ADDR should be configured with the IP address of the partner SWS.

Unlike MTP3 there is no need to specify any further configuration for inter-SWS communication (i.e., inter unit links or linksets), M3UA within the SWS pair will use the inter SWS Ethernet link to maintain communication with the network even when a single SWS loses direct communication to an adjacent Server (signaling Gateway or IPSP).

Dual resilient operation using M3UA does require load-sharing which is based on SLS value. Load-sharing should be configured using the STN_LAS command on both units.

## 9.11 GTT Configuration

Global Title Translation (GTT) is a process used to add or modify information in Global Titles to enable messages to be routed onwards. This may take the form of adding a Point Code or Subsystem Number or modifying the Global Title Address Information.

Typically, GTT examines the Global Title of a Called Party Address and compares it to the rules configured. If the Global Title and Global Title Address Information match, then the translation is performed. The message is then routed accordingly as it passes down the SS7 Protocol stack.

GTT support allows for simple translation of GTAI digits from one number to another. GTT also supports translations using wildcard matching to identify blocks of numbers which require the same translation operation as well as more sophisticated translations which drop or insert blocks of numbers.

Global Title Translation is a function performed by SCCP.

### 9.11.1 How to configure GTT

GTT is performed in two stages. First, the 'match' stage identifies which digits should be matched and which should be ignored, through either single digit or variable length wildcards. The second stage defines the translation operation to be performed. The user can specify to keep the digits in the address being translated, replace them with specified digits, or drop that block of digits.

There are three components to a GTT rule when configured using the config.txt file:

- the Pattern component, which specifies the GT information which must be matched,
- the Address component, which specifies the Address information to use when translating, and

- the GTT Rule component, which controls how the Address Global Title is used during the translation process. The GTT Rule can additionally specify a Backup Address which is used if the first cannot be routed to at that time.

### 9.11.2 Global Title Address Information

GTAI digits may be split up into logical sections using the "/" separator character. Each section will contain zero or more digits.

Each section in the Pattern defines a set of digits which must be matched. Valid digits are in the ranges "0-9", "a-d" and "f". Wild cards may be used where the value of the digits is not significant. The "?" character represents a single digit wildcard, and the "+" character indicates a variable-length wildcard. If no digits are supplied for a section, then the section has no effect on the matched digits. An empty section is used to mark the position in the GTAI digits where digits are inserted from the Address. Padding characters may be added to aid readability.

Each section in the GTT Rule Mask defines how the replacement operation is performed. Sections marked "K" identify that the section of the Called Address being translated should be kept. Sections marked "R" identify that the section of the Called Address being translated should be replaced with digits from the Address component referenced by the GTT Rule. GTT Rule sections should not be empty.

### 9.11.3 Examples

#### 9.11.3.1 Example 1

- Match GTAI digits 09876543210.
- Remove the GTAI and add a PC (138) and SSN (8).

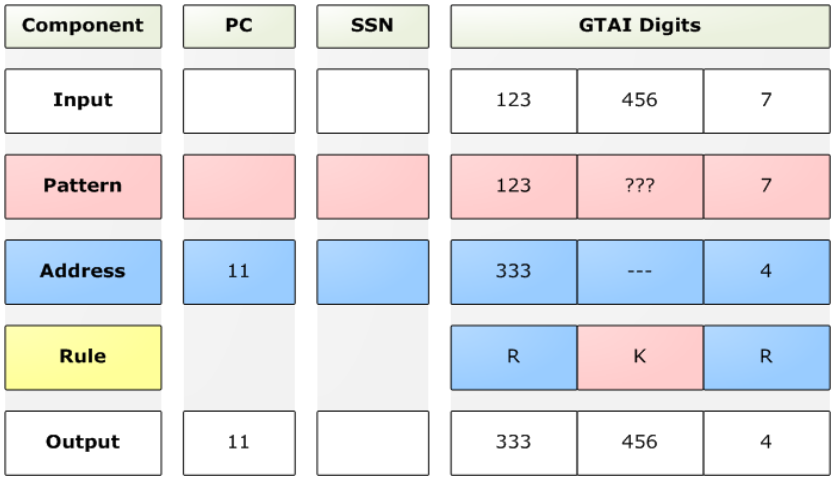
| Component | PC | SSN | GTAI Digits |
|---|---|---|---|
| Input | | | 09876543210 |
| Pattern | | | 09876543210 |
| Address | 138 | 8 | - |
| Rule | | | R |
| Output | 138 | 8 | |

```
*
*  Specific Address to PC + SSN
*  This example translates a received specific Global Title address (09876543210) into a
*  combination of Point Code (138) and SSN (8).
*
* SCCP_GTT_PATTERN <pattern_id> <addr_indicator> <pc>     <ssn> <global_title> [<gtai_pattern>]
SCCP_GTT_PATTERN   11            0x10             0        0     0x001104       09876543210
*
*
*SCCP_GTT_ADDRESS [<nc_id>]<address_id><addr_indicator><pc><ssn><global_title><gtai_replacement>]
SCCP_GTT_ADDRESS            11          0x03           138  8    0             -
*
*
*SCCP_GTT [<nc_id>] <pattern_id> <mask><primary_address_id> [<backup_address_id>]
SCCP_GTT            11            R     11
*
```

#### 9.11.3.2 Example 2

- Match a seven digit number starting "123", followed by any three digits, then "7".

- Change the first digits to "333". Keep the next three digits from the called-party address. Change the fourth digit to "4". Add a PC (11).



| Component | PC | SSN | GTAI Digits | | |
|---|---|---|---|---|---|
| Input | | | 123 | 456 | 7 |
| Pattern | | | 123 | ??? | 7 |
| Address | 11 | | 333 | --- | 4 |
| Rule | | | R | K | R |
| Output | 11 | | 333 | 456 | 4 |

```
* Match a 7 digit number starting "123", followed by any three digits, then "7".
* change the first digits to "333" keep the next three digits from the called-party
* address and change the fourth digit to "4", and add a PC (11).
*
* SCCP_GTT_PATTERN <pattern_id> <addr_indicator> <pc>     <ssn> <global_title> [<gtai_pattern>]
SCCP_GTT_PATTERN    6            0x10             0x0000   0     0x001104       123/???/7
*
*
*SCCP_GTT_ADDRESS [<nc_id>]<address_id><addr_indicator><pc><ssn><global_title><gtai_replacement>]
SCCP_GTT_ADDRESS            2           0x11             11  0    0x001104      333/---/4

**
*SCCP_GTT [<nc_id>] <pattern_id> <mask>      <primary_address_id> [<backup_address_id>]
SCCP_GTT            6             R--/K--/R   6
```

### 9.11.3.3 Example 3

- Match "441425", followed by any digits.
- Remove the first six digits. Keep any following digits in the Input GTAI. Add a PC(238) & SSN (3).

| Component | PC | SSN | GTAI Digits | |
|---|---|---|---|---|
| Input | | | 441425 | 123456 |
| Pattern | | | 441425 | + |
| Address | 238 | 3 | - | - |
| Rule | | | R | K |
| Output | 238 | 3 | | 123456 |

```
* A Matching Prefix to PC + SSN
*  This example translates any global title address matching a pattern consisting of a
*  prefix (441425) following by a suffix of any digits and any length into
*  a combination of Point Code (235) and SSN (3).
*
* SCCP_GTT_PATTERN <pattern_id> <addr_indicator> <pc>     <ssn> <global_title> [<gtai_pattern>]
SCCP_GTT_PATTERN   12            0x10             0        0     0x001104       441425/+
*
*
*SCCP_GTT_ADDRESS [<nc_id>]<address_id><addr_indicator><pc><ssn><global_title><gtai_replacement>]
SCCP_GTT_ADDRESS            12          0x03            238 3    0              -/-
*
*
*SCCP_GTT [<nc_id>] <pattern_id> <mask>      <primary_address_id> [<backup_address_id]
SCCP_GTT             12           R/K         12
```

### 9.11.3.4 Example 4

- Match a GT with any GTAI Digits.
- Keep any digits which are present and add a PC and SSN.

| Component | PC | SSN | GTAI Digits | |
|---|---|---|---|---|
| Input | | | 12345 | |
| Pattern | | | + | - |
| Address | 128 | 8 | - | - |
| Rule | | | K | R |
| Output | 128 | 8 | 12345 | |

```
* Adding a PC + SSN to any GTAI
* This example matches any GTAI Digits and adds a Point Code and SSN, retaining any GTAI digits.
*
* SCCP_GTT_PATTERN <pattern_id> <addr_indicator> <pc>     <ssn> <global_title> [<gtai_pattern>]
SCCP_GTT_PATTERN    1            0x10             0x0000    0x03   0x001204       +/-
*
*
*SCCP_GTT_ADDRESS [<nc_id>] <address_id> <addr_indicator> <pc>     <ssn> <global_title>
<gtai_replacement>]
SCCP_GTT_ADDRESS             1            0x53             0x3FFF    0x08   0x001204       -/-
*
*
*SCCP_GTT [<nc_id>] <pattern_id> <mask> <primary_address_id> [<backup_address_id]
SCCP_GTT             1            K/R    1
```

## 9.12 HSL Signaling

The SIU supports both structured (framed) and un-structured HSL links in accordance with *ITU Q.703, Annex A*.

HSL links can be configured on systems employing Dialogic® DSI SS7HDP Network Interface Boards, which support up to 2 HSL links per board or 6 HSL links per unit.

### 9.12.1 LIU_CONFIG

The LIU_CONFIG command <frame_format> parameter should be given a value of 10 - when configuring unstructured high speed links.

### 9.12.2 MTP_LINK <interface_mode>

The MTP_LINK command supports a new parameter, <interface_mode>, that identifies the interface type for signaling links.

The interface mode should be set to one of the following values:

| Interface_mode | Description |
|---|---|
| TDM | Single timeslot signaling link |
| E1_HSL | Unstructured E1 HSL operation.<br>***Note:*** LIU frame_format must be set to 10. |
| T1_HSL | Unstructured T1 HSL operation.<br>***Note:*** LIU frame_format must be set to 10. |
| E1_FRAMED | Framed 31 timeslot E1 operation |
| T1_FRAMED | Framed 24 timeslot T1 operation |
| E1_PCM | Structured 30 timeslot E1 operation (timeslots 0 and 16 are used for signaling) |

The interface_mode value must be consistent with the liu_type and frame_format values of the LIU_CONFIG command.

### 9.12.3 MTP_LINK <flags>

| Bit number | Description |
|---|---|
| 10 & 11 | Set both to zero for E1_HSL and T1_HSL operation.<br>HSL framed operation uses these bits in a similar manner to single timeslot signaling to select 64 Kbps, 56 Kbps or 48 Kbps operation that applies to all timeslots within the HSL link. |
| 12 | Sequence number length. Set to 1 the HSL signaling link will use a 12bit sequence number. If set to 0, the HSL signaling link will use a 7bit sequence number. |

### 9.12.4 MTP_LINK <timeslot>

For HSL links, the <timeslot> parameter should be set to **0xff** to indicate that the link is attached to an LIU configured with the LIU_CONFIG command.

HSL signaling links might not use timeslots already configured for signaling or data. TDM links might not use timeslots already configured for HSL or data.

### 9.12.5 MTP_LINK <blink>

For HSL links the signaling processor channel of the **<blink>** parameter must be set to a value of 0. Only values 0-0 and 1-0 are permitted.

On each Dialogic® DSI SS7HDP Network Interface Board, a single processor cannot be configured for both HSL and TDM links. Different processors on the same SS7HDP board can be used individually for HSL and non-HSL operation.

## 9.13 ATM Signaling

ATM signaling on the SS7G32 is supported through the field installation of up to 2 Dialogic® SS7MD Network Interface Boards. SS7MD boards cannot be installed in a SS7G31 or SS7G2x Signaling server. See the Signaling Servers User Manual Supplement for ATM Operation for further information regarding ATM signaling.

# Glossary

| | |
|---|---|
| A-link | An “access” link that connects a signaling end point (for example, an SCP or SSP) to an STP. Only messages originating from or destined to the signaling end point are transmitted on an A-link. |
| AIS | Alarm Indication Signal (Blue alarm). |
| API | Application Programming Interface |
| BER | Bit Error Rate. |
| blink | The index of the logical signaling processor (SP) channel (within the board) allocated for a signaling link. For Dialogic® DSI SPCI4 Network Interface Boards that have a single processor that supports 4 signaling links the blink parameter is a single value in the range 0 to 3. For Dialogic® DSI SS7HDP Network Interface Boards that have two signaling processors with each processor supporting up to 32 signaling links, the blink parameter is a compound parameter of the form x-y, where x represents the processor (a value of 0 or 1) and y represents the SS7 signaling processor (SP) channel within the processor (a value in the range 0 to 31). |
| CCITT | Consultative Committee on International Telegraphy and Telephony |
| config.txt | A text file used for protocol configuration. |
| CPU | Central Processing Unit |
| CSSR | A concerned SCCP sub-system resource, that is, a sub-system resource that wants to receive state change information about another SCCP sub-system or signaling point. |
| DPC | Destination Point Code. Identifies the address (point code) of the SS7 network node to which a Message Signal Unit (MSU) should be directed. |
| DSI | Distributed Signaling Interface. |
| dual resilient | A term used to describe a system that consists of two SIUs configured as a single point code in the SS7 network. Under normal circumstances, both SIUs share the load. If one unit fails, the partner unit maintains operation of the node. |
| F-link | An “fully-associated” link that connects two signaling end points (for example, SSPs and SCPs). F-links are not usually used in networks with STPs. In networks without STPs, F-links directly connect signaling points. |
| FTP | File Transfer Protocol |
| gctload | A program that handles the initialization sequence and creates inter-process communication. |
| HTTP | The Hypertext Transfer Protocol (HTTP) is a protocol used extensively to provide the application-level communication between client and servers in web and web-service enviroments |
| MAP | Mobile Application Part (MAP). An SS7 stack layer supporting messages sent between mobile switches and databases to support user authentication, equipment identification, and roaming. |
| MTP | Message Transfer Part. Layers 1 to 3 of the SS7 protocol stack broadly equivalent to the Physical, Data Link and Network layers in the OSI protocol stack. See also MTP1, MTP2, and MTP3. |
| MSU | Message Signal Unit. A data unit that carries signaling information for call control, transaction processing, network management and maintenance. Typically, the MSU is carried in the Signaling Information Field (SIF) of SS7 messages. |
| LIU | Line Interface Unit. |
| Link | A physical and logical connection between two signaling points. |
| Link set | One or more signaling links that are connected to adjacent signaling points. |

| | |
|---|---|
| mtpsl | An example utility that can also be used to activate and deactivate signaling links. |
| OPC | Originating Point Code. A signaling point code that identifies the signaling point at which a message originated. |
| RAI | Remote Alarm Indication (Yellow alarm). |
| REST | Repesentational State Transfer. An architetural style applied widely in web-service APIs. |
| route | An MTP3 concept that determines how signaling is distributed over link sets. A route consists of a destination point code and the link set ID of one or two link sets over which traffic to the destination node should be routed. When two link sets are provided, you can choose to load share traffic or treat the link sets as primary and secondary. |
| rsi | A process manages the connection between the host and each SIU. It takes several command line parameters and is normally spawned by an entry in the host's system.txt file. |
| rsicmd | A command that starts the Ethernet link between a host and an SIU. |
| s7_play | A utility that can be used to generate messages from a text file and send them to the system. Typically used for diagnostic purposes. |
| s7_log | A utility that enables messages received from the protocol stack to be logged in a text file. Typically used for diagnostic purposes. |
| SCCP | Signal Connection Control Part. An SS7 stack layer that allows a software application at a specific node in an SS7 network to be addressed. |
| SGW | Signaling Gateway |
| SIU | Signaling Interface Unit |
| SP | Signaling Processor |
| SP channel | The logical processing channel, within the signaling processor hardware, that conducts the processing of a signaling link. |
| SS7 | Signaling System Number 7 |
| SS7HD | An identifier for the family of Dialogic® DSI High Density SS7 Network Interface Boards. |
| SS7 Protocol Stack | A set of software modules that implement the various layers of the SS7 protocol stack. |
| SSH | Secure Shell |
| SSP | Service Switching Point |
| STP | Signaling Transfer Point |
| SSR | An SCCP sub-system resource. This can be a local sub-system, a remote sub-systems or a remote signaling point. |
| system.txt | A text file used for system configuration. |
| TCAP | Transaction Capabilities Application Part. An SS7 stack layer that enables the deployment of intelligent network and mobile services by supporting non-circuit related information exchange between signaling points using the SCCP connectionless service. |
| ttu | An example program that demonstrates how a user application can interface with the TCAP protocol module. |
| timeslot | The smallest, switchable data unit on a TDM bus. For T1 and E1 technologies, one time slot is equivalent to a data path with a bandwidth of 64 Kbps. |
| upe | A worked example of exchanging messages with the MTP3 module. |